NDI

Análisis de datos para el monitoreo de redes sociales

Guía sobre técnicas, herramientas y metodologías de monitoreo y análisis de redes sociales

Mayo 2020

Índice temático

Autores

Nick Monaco es director del Laboratorio de Inteligencia Digital (DigIntel) del Instituto para el Futuro (*Institute for the Future*). Es experto en desinformación en línea y el uso de bots políticos y especialista en desinformación china. En el transcurso de su trabajo ha asesorado a responsables de formular políticas y a tecnólogos, tanto del gobierno como de la industria, sobre la mejor manera de combatir la desinformación y mantener la integridad electoral en países de todo el mundo. Anteriormente trabajó en estas cuestiones en Graphika, una empresa dedicada al análisis de redes sociales e inteligencia de amenazas, así como en Jigsaw, el grupo de expertos (*think-tank*) en derechos digitales de Google. También es investigador asociado en el Proyecto de Propaganda Computacional (ComProp) del Instituto de Internet de Oxford (*Oxford Internet Institute*).

Daniel Arnaudo trabaja en el NDI como asesor de estrategias de información, a cargo de la intersección de la democracia y la tecnología, con la responsabilidad especial de desarrollar programas que rastreen la desinformación y promuevan la integridad de la información en todo el mundo. Al mismo tiempo, es becario del programa de Ciberseguridad de la Escuela de Estudios Internacionales Jackson de la Universidad de Washington, donde ha trabajado en proyectos en Brasil, Myanmar y Estados Unidos. Recientemente, también colaboró con el grupo de investigación del Instituto de Internet de Oxford en el área de propaganda computacional. Su investigación se enfoca en campañas políticas en línea, derechos digitales, ciberseguridad y tecnologías de la información y comunicación para el desarrollo.

Acerca del NDI

El Instituto Nacional Demócrata para Asuntos Internacionales (NDI) es una organización no gubernamental sin fines de lucro y apartidista que responde a las aspiraciones de personas de todo el mundo que desean vivir en sociedades democráticas que reconozcan y promuevan los derechos humanos básicos.

Desde su fundación en 1983, el NDI y sus aliados locales han trabajado para apoyar y fortalecer las instituciones y prácticas democráticas mediante el fortalecimiento de los partidos políticos, las organizaciones de la sociedad civil y los Parlamentos, así como la salvaguarda de las elecciones y la promoción de la participación ciudadana, la apertura y la rendición de cuentas de los gobiernos.

Al contar con personal y actores políticos voluntarios de más de 100 naciones, el NDI reúne a personas y grupos para compartir ideas, conocimientos, experiencias y pericia. Las organizaciones aliadas tienen la oportunidad de conocer de cerca las mejores prácticas de desarrollo democrático internacional que pueden adaptarse a las necesidades de sus propios países. El enfoque multinacional del NDI reafirma el mensaje de que, si bien no existe un modelo democrático único, todas las democracias comparten ciertos principios medulares.

El trabajo del Instituto propugna por los principios consagrados en la Declaración Universal de los Derechos Humanos. También promueve el desarrollo de canales de comunicación institucionalizados entre los ciudadanos, las instituciones políticas y los funcionarios elegidos, al tiempo que fortalece su capacidad de mejorar la calidad de vida de toda la ciudadanía. Para obtener más información acerca del NDI, visite la página www.ndi.org.

Agradecimientos

El Instituto agradece el apoyo de la Fundación Nacional para la Democracia (NED, por sus siglas en inglés) en el financiamiento de la creación de esta guía. La NED es una fundación privada sin fines de lucro dedicada al crecimiento y fortalecimiento de las instituciones democráticas en todo el mundo. Cada año, la NED otorga más de 1,600 subvenciones para apoyar los proyectos de grupos no gubernamentales en el extranjero que trabajan por objetivos democráticos en más de 90 países. Desde sus inicios en 1983, la Fundación se ha mantenido a la vanguardia de las luchas democráticas en todas partes, a la vez que evoluciona para convertirse en una institución multifacética que funciona como centro de actividades, recursos e intercambio intelectual para activistas, profesionales y académicos de la democracia de todo el mundo.

El NDI también reconoce al Instituto para el Futuro (IFTF, por sus siglas en inglés) por su cooperación y alianza en la distribución de esta guía. El IFTF es una organización sin fines de lucro dedicada al futuro cívico; es la organización líder en el mundo en cuestiones del futuro. Durante más de 50 años, empresas, gobiernos y organizaciones de impacto social han dependido de los pronósticos mundiales, la investigación personalizada y la capacitación en previsión que ofrece el IFTF para navegar los complejos cambios y desarrollar estrategias que estén listas para el mundo. Las metodologías y los conjuntos de herramientas del IFTF producen visiones coherentes de las posibilidades de transformación en todos los sectores que, en conjunto, respaldan un futuro más sostenible.

Diseño e impresión: Ironmark, 2020

Introducción

Las redes sociales se han convertido en una parte cada vez más importante de las conversaciones que las y los ciudadanos(as), candidatos(as), partidos y organizaciones relacionadas(os) entablan en torno a eventos políticos, elecciones y referéndums, así como para votar proyectos de ley, convocar huelgas y llevar a cabo otras formas de actividad política. Es fundamental que los investigadores, los observadores electorales, las organizaciones de la sociedad civil y la gente común y corriente se equipen con herramientas, métodos y prácticas para ayudar en la recopilación y el análisis de datos del espacio en línea. Los miembros de organizaciones internacionales de la sociedad civil, incluyendo investigadores, gerentes de programas, activistas y otros, participan en diversos programas a nivel internacional, incluso como parte de misiones de observación electoral, con el fin de apoyar a los grupos locales a desarrollar su propia capacidad de monitoreo, o monitorear el discurso de odio, las tendencias políticas y una gran cantidad de cuestiones adicionales.

Esta es una guía para ayudar a los investigadores, observadores electorales, tecnólogos y demás personas relacionadas a comprender las mejores prácticas, herramientas y metodologías para desarrollar la observación y el monitoreo en línea de las redes sociales. Presenta una introducción a los conceptos relevantes para una mejor comprensión del estudio de estos temas, así como una revisión de cómo crear una imagen completa del contexto socio-técnico en un país o región, incluyendo la presencia en línea de los partidos locales, las redes sociales y los índices de penetración del Internet, los medios de comunicación locales, las divisiones étnicas y religiosas y una serie de factores adicionales que se manifiestan en el espacio en línea.

Esta guía contiene información sobre los siguientes temas clave:

- ***Colaboración:*** Los investigadores deben considerar socios potenciales y formas de elegirlos, ya sean distintos tipos de organizaciones locales, ONGs internacionales con experiencia en el área o empresas privadas que van desde las más pequeñas con experiencia en el campo hasta grandes corporaciones multinacionales que controlan plataformas de redes sociales y otras tecnologías que llegan a las redes mundiales. En una sección de esta guía se analizan las posibles opciones y consideraciones para estas colaboraciones, se citan ejemplos y se señalan los beneficios y riesgos de trabajar con diferentes grupos.
- ***Metodología:*** En cuanto a la metodología, en la guía se analizan los diferentes métodos de recopilación de datos, incluyendo las consideraciones para las distintas plataformas, los métodos para trabajar con las interfaces de programación de aplicaciones (API, por sus siglas en inglés) de cada una, y para extraer contenido de diferentes maneras.
- ***Mapeo y visualización:*** Esta sección ofrece orientación sobre el desarrollo y la lectura de mapas de redes. La guía presenta términos técnicos clave, así como métodos para construir mapas del espacio en línea, ejemplos de la investigación de campo, y posibles limitaciones de los mapas en sí.
- ***Análisis:*** En esta sección se analizan los diferentes tipos de entidades e individuos que dan forma a la conversación. La guía sobre este tema incluye una descripción general de las cuentas individuales, las personas influyentes (*influencers*) y los grupos, así como el papel que desempeña cada uno de ellos en el ecosistema en línea; asimismo, se analizan las distintas maneras en que las organizaciones de noticias y otros recursos externos se convierten en fuentes importantes de contenido.
- ***Contenido:*** Al abordar el contenido en línea, la guía analiza diferentes aspectos de las publicaciones (*posts*), los tuits y otras formas de redes sociales. En esta sección se describe cómo detectar diferentes tipos de propaganda computacional en las redes, que van desde botnets (redes de robots informáticos) y granjas de troles (*trolls*), hasta otras formas potenciales de manipulación. Se consideran varias formas maliciosas de contenido manipulador que van desde la desinformación hasta el discurso de odio y sus posibles objetivos.
- ***Herramientas:*** Para apoyar estas técnicas de investigación, la guía cataloga y analiza los diferentes tipos de herramientas que son útiles en el desarrollo del análisis de varios aspectos del monitoreo de las redes sociales. Este inventario incluye herramientas para la recopilación en diversas plataformas, así como recursos para el análisis de redes, visualización de datos e investigación de inteligencia de fuentes abiertas.
- **Respuestas:** Finalmente, la guía presenta una revisión de posibles respuestas que pueden beneficiarse de la información obtenida de estos análisis y por lo tanto, mejorarse. Esto incluye la recopilación de datos para la investigación, el desarrollo de documentación, y la creación de mecanismos para la elaboración de informes en colaboración con plataformas, reguladores del gobierno y organizaciones de monitoreo electoral. La guía concluye con recomendaciones para llevar a cabo investigaciones en áreas futuras y desarrollar evaluaciones críticas de áreas del campo en evolución.

Antecedentes

Al ingresar a un nuevo entorno, los analistas deben considerar muchos actores, redes y grupos sociopolíticos, así como también sistemas técnicos. Deben analizar varios aspectos de los ámbitos informativos, sociales y políticos en los que están trabajando, considerando las redes y la organización del país en sí, la región más amplia y su lugar en el sistema global. La información no siempre se transmite a través de redes de medios tradicionales o en línea; gran parte de esto existe de boca en boca, a través de rumores, medios tradicionales y otros métodos. Sin embargo, hoy en día, a menudo estas conversaciones se permean en línea, donde pueden rastrearse y comprenderse mejor.

Varios grupos a nivel internacional emplean tácticas para manipular la percepción pública sobre los candidatos y problemas, debilitar la confianza en los procesos democráticos y confundir a los votantes sobre la ubicación de las casillas electorales, su registro o el sistema electoral en sí. Uno de los propósitos centrales de este tipo de investigación es ayudar a tener una idea más clara de la manera en que las redes de propaganda computacional[1] operan en línea, ayudando así a exponer cómo funcionan, documentar casos para investigación y potencialmente alertar a las autoridades o compañías de redes sociales sobre la manipulación y el abuso en línea. La detección de la automatización, las cuentas falsas, el contenido falso, las malas fuentes de información y otros tipos de manipulación podría ser el objetivo de este tipo de proyectos para describir la propaganda computacional en diferentes casos.

Los analistas de las redes sociales que revisan los problemas de información en contextos de todo el mundo deben tener en cuenta muchos factores cuando elaboran sus informes. Deben desplegar herramientas, investigar sobre las leyes e instituciones que rigen el espacio de información y emplear métodos en persona, como entrevistas con funcionarios de gobierno, partidos, medios de comunicación y candidatos(as), para crear una imagen más precisa de la desinformación en el entorno electoral.

La desinformación es un tema difícil de captar porque generalmente no es un término que esté muy bien definido. Un componente clave de la desinformación es el concepto de intención, ya que la desinformación se transmite con la intención de engañar, mientras que la información errónea es contenido incorrecto sin que necesariamente se tenga la intención de falsificarlo. Para obtener más información sobre las definiciones y más antecedentes sobre estos temas, consulte el informe de Data & Society, *Lexicon of Lies* [Léxico de mentiras], y el documento de First Draft, *Information Disorder* [Desorden de la información], así como la guía del NDI, *Apoyando la integridad de la información y el discurso político civil*[2], que se ha traducido al albanés, árabe, inglés, francés, ruso, serbio y español. En la sección de referencias se indican fuentes adicionales. Además de la desinformación, un investigador debe considerar muchos tipos distintos de contenido, tanto los que son inocuos, como los maliciosos y los positivos.

También es importante considerar el papel de los medios y la manera en que operan dentro de los sistemas de redes sociales y en línea e influyen en ellos. Revise las principales fuentes de publicaciones impresas, radio y televisión y evalúe su participación en el mercado, los vínculos con los partidos políticos, la participación de los sectores público y privado y la manera en que influyen en el espacio en línea. Muchos de ellos tienen una presencia en línea considerable y, particularmente cuando están vinculados con un partido político importante, pueden tener una gran influencia en la línea editorial y las preferencias políticas de una organización, así como la tendencia a obtener apoyo viral, ya sea orgánico o generado artificialmente. La polarización en este contexto puede verse como algo crítico en relación con las redes, y puede hacerse evidente cuando se forman grupos más grandes y distintos en la oposición y la coalición, lo cual también puede indicar los niveles de propaganda computacional y desinformación que están presentes.

El discurso de odio a menudo incluye desinformación para difamar a los objetivos de las campañas con ataques falsos. Esto se dirige particularmente a mujeres, minorías y otros grupos vulnerables. La investigación del equipo de Género, Mujeres y Democracia del NDI sobre la violencia contra las mujeres en la política (VAW-P, por sus siglas en inglés) señala que "cuando los ataques contra mujeres políticamente activas se canalizan en línea, el alcance expansivo de las plataformas de redes sociales aumenta los efectos del abuso psicológico al hacer que esos efectos parezcan anónimos, sin fronteras y sustentados, lo que debilita el sentido de seguridad personal de las mujeres en formas que los hombres no experimentan. Muchos de los actores dentro y fuera del gobierno que cometen VAW-P en línea se movilizan a través de redes transnacionales. El mal uso que hacen los estados, las organizaciones y los individuos de las libertades que se supone que el espacio de información debe permitir, se ha convertido en una de las mayores amenazas para su integridad". (Zeiter et al., 2019, 4) Como resultado, los investigadores

1 Según el Instituto de Internet de Oxford, cuyo grupo de investigación ayudó a definir el término y fue pionero en gran parte de la investigación en torno a estos temas: "La propaganda computacional es el uso de algoritmos, automatización y selección o curación de contenidos por humanos para distribuir intencionalmente información engañosa en las redes sociales" (Woolley y Howard, 2017, 4).

2 Consulte https://www.ndi.org/publications/supporting-information-integrity-and-civil-political-discourse

deben ser conscientes de la manera en que las mujeres son especialmente vulnerables a estos ataques en línea y considerar formas de documentar y denunciar a las plataformas este tipo de abuso. El NDI ha puesto a prueba el uso de léxicos de términos del discurso de odio para examinar las redes sociales con estudios de casos en Colombia, Indonesia y Kenia. Los métodos para el desarrollo de estos léxicos y los estudios de caso se detallan en el informe de esta investigación: "*Tweets that Chill: Analyzing Violence Against Women in Politics* [Tuits que dan escalofríos: Análisis de la violencia contra las mujeres en la política].

Al desarrollar estrategias para la recopilación de datos, considere la manera en que estas operaciones de información que utilizan el discurso de odio y la propaganda computacional operan dentro del contexto en el que usted está trabajando. Los siguientes contenidos de esta guía ayudarán a los analistas a aprender a identificar estas campañas, redes y usuarios en línea, pero antes de proceder, los investigadores deben entender ampliamente qué tipo de propaganda computacional, discurso dañino u otros patrones están buscando.

También es importante tener una comprensión general tanto del entorno regulatorio local (incluyendo las leyes electorales y de financiamiento de campañas, lo cual puede ayudar a la elaboración de los informes), como de las reglas de moderación de contenido y las políticas que rigen las plataformas que se estudian. Lo anterior a fin de que los investigadores puedan diseñar sus estudios de manera legal y ética y alertar a las empresas, y posiblemente a los gobiernos, sobre el abuso y otras acciones ilegales y negativas en línea. Esto también ayuda a los investigadores a comprender mejor a los países que estudian.

Entender los términos de servicio de las distintas compañías de redes sociales representa un aspecto crucial de estos informes. A continuación se enumeran las normas clave para este entendimiento de Facebook, Twitter y YouTube y se incluyen los vínculos a sus políticas.

Normas comunitarias de Facebook	▪ Información importante sobre cómo reportar distintos hechos, aquí. ▪ "Reportar una página de impostor de una figura pública" aquí. ▪ "Cómo reportar contenido" desglosado por tipo de publicación, aquí. ▪ "¿Cómo indico que una publicación es una noticia falsa?", aquí.
Reglas de Twitter	▪ Panorama general sobre cómo denunciar un incumplimiento, aquí. ▪ Cómo denunciar un tuit, una cuenta con contenido abusivo o un mensaje individual aquí. ▪ Denunciar cuentas de suplantación de identidad, aquí. ▪ Instrucciones para denunciar spam, aquí.
Lineamientos de la comunidad YouTube	▪ Cómo denunciar contenido inapropiado, desglosado por tipo de publicación, aquí. ▪ "Cómo denunciar una predicción de búsqueda de YouTube", aquí. ▪ "Otras opciones para denunciar", aquí. ▪ "Cómo denunciar spam o contenido engañoso" aquí (final de la página). ▪ Herramienta de YouTube para hacer denuncias, aquí.

Algunas compañías, como Facebook, requieren que los usuarios se identifiquen con información real, por lo que el simple hecho de identificar una cuenta que no sea de una persona real, o un grupo conectado a esa cuenta falsa, puede hacer que se elimine. Otras, como Twitter, no prohíben el anonimato, pero sí el discurso de odio o la amplificación artificial que pueden identificarse y denunciarse mediante investigaciones. Vale la pena familiarizarse con los distintos códigos y mecanismos para denunciar contenido que se describen en la tabla anterior.

Denunciar es importante, al igual que documentar las campañas, las cuentas y el contenido relevante para que puedan verificarse las denuncias. Considere el uso de sistemas que puedan respaldarse y consultarse fácilmente en cuanto a anotaciones y flujos de trabajo. Como se mencionó anteriormente, las normas comunitarias de Facebook ofrecen mecanismos para reportar cuentas falsas y formas negativas de contenido, así como para solicitar que se verifique y posiblemente se elimine contenido dañino. Las reglas de Twitter permiten distintas maneras de denunciar la suplantación de identidad, el spam y ciertas formas de discurso de odio o prohibido. Las políticas de YouTube se enfocan en los medios de comunicación y derechos de autor, así como en contenido explícito, de odio u otras formas dañinas de expresión. Como propietarios de YouTube, los

términos de referencia de Google nos dan una idea, no solo de la manera en que se pueden denunciar las cuentas, sino también de cómo se pueden investigar aquellas cuentas vinculadas al servicio de transmisión de video en directo (*streaming*).

En términos de regulaciones gubernamentales, los analistas deben considerar las leyes de protección de datos, como el Reglamento General de Protección de Datos de la Unión Europea, el cual contiene aspectos que cubren la recopilación de información de identificación personal en Europa o sobre europeos en cualquier lugar, así como las empresas que operan allí.[3] La recopilación de datos provenientes de grupos, usuarios y redes privadas(os) podría derogar dichas leyes, así como los términos de servicio de las plataformas.

Redes como la Coalición Design 4 Democracy (Coalición D4D) pueden ayudar a abogar por los principios democráticos en las empresas de tecnología, por ejemplo, para atraer la atención de las plataformas hacia las campañas de influencia a mayor escala para campañas electorales, los discursos de odio o para otros fines. La Coalición D4D está formada por organizaciones de la sociedad civil nacionales e internacionales que trabajan en conjunto con compañías tecnológicas para integrar y apoyar los principios democráticos, incluso en el contexto de moderación de contenido, desarrollo de políticas y consideraciones de productos. La Coalición (con el liderazgo del NDI, el Instituto Republicano Internacional, la Fundación Internacional para Sistemas Electorales e IDEA Internacional) vincula a las partes interesadas de la sociedad civil y la democracia en diversos contextos con muchas de las compañías tecnológicas más influyentes (incluyendo Facebook, Microsoft y Twitter) a fin de fomentar el intercambio de información y suscitar estrategias para promover la integridad de la información y proteger los procesos democráticos. Esfuerzos como estos se pueden respaldar y mejorar mediante documentación, análisis e informes sólidos utilizando las herramientas, los métodos y las tácticas que aquí se describen.

Para obtener más detalles sobre el desarrollo de estrategias para el análisis de datos en las redes sociales durante las elecciones, consulte el documento de orientación del NDI sobre Desinformación e Integridad Electoral [*Disinformation and Election Integrity*][4], así como la Guía de Apoyo a la Democracia para la Sociedad Civil sobre el Monitoreo de las Redes Sociales para las Elecciones [*Supporting Democracy's Guide for Civil Society on Monitoring Social Media for Elections*].[5] Estas guías incluyen metodologías y consideraciones regulatorias para los observadores en cuanto a monitoreo de redes sociales y la posibilidad de integrar los datos recopilados en línea en las misiones tradicionales de observación de elecciones.

Cómo trabajar con la recopilación de datos

La recopilación de datos es el primer paso para un análisis riguroso de la actividad en línea en torno a una elección. Como analista de campo, el primer paso para recopilar datos es realizar un sondeo del panorama de las redes sociales o en línea en la región que está observando. Las preguntas importantes a considerar incluyen:

- ***¿Qué plataformas son las más populares en la región? ¿Cuáles son los índices de penetración de las distintas plataformas?*** Internet World Stats, la Unión Internacional de Telecomunicaciones, el informe sobre la libertad en la red de Freedom House, o el propio Facebook pueden ser buenas fuentes en este caso. Un país con altas tasas de participación en Facebook pero bajos índices de penetración en Twitter (como Taiwán), probablemente producirá ideas más valiosas en Facebook.
- ***¿Qué sitios web son populares para las noticias? ¿Cuáles de estos son medios de tradición? ¿Cuáles de estos son de creación más reciente?***
- ***¿Qué etiquetas (hashtags) son más relevantes para la elección en cuestión? Del mismo modo, ¿qué cuentas oficiales representan a los partidos, candidatos(as) y sus campañas en estas elecciones?*** A menudo, un(a) candidato(a) tendrá más de una cuenta o página relevante para una elección, como una cuenta personal de Twitter y una cuenta oficial de la campaña en Twitter. Hacer una lista de todo esto es un buen primer paso para recopilar datos relevantes.

Después de distinguir las plataformas y los sitios web de redes sociales más importantes del país, ya está listo(a) para comenzar a recopilar datos en plataformas y sitios web relevantes. En esta sección analizaremos las opciones que los investigadores tienen a su disposición para la recopilación de datos.

3 https://gdpr.eu/
4 https://www.ndi.org/publications/disinformation-and-electoral-integrity-guidance-document-ndi-elections-programs
5 La guía *Supporting Democracy* la implementa un consorcio conformado por SOFRECO, Democracy Reporting International (DRI) y el NDI. https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf

Métodos de recopilación

Los investigadores tienen varias opciones disponibles para recopilar datos de redes sociales en línea. Las tres principales son utilizar herramientas de recopilación de terceros, interactuar directamente con la API de alguna plataforma o extraer datos de la web y almacenarlos en una base de datos (*web scrapping*). En esta sección analizaremos las características de cada uno de estos métodos y las diferencias que existen entre ellos.

Herramientas de terceros (acceso indirecto)

Para los investigadores que deben cumplir con plazos ajustados o que no tienen la capacidad de interactuar con sitios web a través de un código de computadora, las herramientas de terceros pueden ser una opción útil. Estas herramientas suelen interactuar con las API de una o más plataformas objetivo de forma invisible en segundo plano y presentan los datos con un diseño gráfico fácil de usar, como una pantalla principal. En el caso de Facebook, que actualmente no permite que investigadores externos o empresas usen su API, CrowdTangle es una de las mejores opciones para monitorear el alcance de las páginas, los grupos y el URL en Facebook, y también les muestra a los usuarios el alcance de los URL en Twitter, Instagram y Reddit. La extensión CrowdTangle[6] le permite al usuario ver en tiempo real una estimación del número de reacciones que una publicación, página o URL ha generado en estas plataformas, lo cual puede ser una manera útil de monitorear diariamente contenido tendencia en múltiples plataformas.

Ciertas herramientas de terceros, como Sysomos y Brandwatch, requieren pagos de suscripciones costosas para poder utilizarlas, pero ofrecen acceso a una gran cantidad de datos que pueden ser útiles para monitorear campañas de etiquetas (hashtags) y otros contenidos que sean tendencia en las redes sociales.

Además de visualizarse en un navegador de Internet, los datos de estas herramientas a menudo se pueden exportar a un archivo legible por máquina, como un archivo de valores separados por comas (CSV, por sus siglas en inglés), que a su vez puede ser manipulado por un científico de datos para consultar los datos de formas nuevas y útiles.

Facebook: Sysomos, Brandwatch
Twitter: Twitonomy

Acceso directo - API y extracción de datos de sitios web ¿Cuál es la diferencia?

Para una interacción más directa con plataformas y sitios web, los investigadores tienen dos opciones disponibles: usar una interfaz de programa de aplicación (API) o recopilar la información directamente del código fuente de la página web, una práctica conocida comúnmente como *extracción de datos de sitios web o "web scrappping"*, su término en inglés. Es importante tener en cuenta la diferencia entre API y la extracción de datos de sitios web: en la mayoría de los casos, extraer datos de las API es legal y ético, ya que los datos de las API están regulados deliberadamente por las plataformas y estructurados de manera que no violan los derechos de los usuarios. Por su parte, la extracción de datos de sitios web es, en muchos casos, una violación de los Términos de Servicio y es más difícil de regular, por lo que puede ser ilegal.

Es importante tener en cuenta la diferencia entre estos dos métodos de recopilación de datos, así como saber que ocasionalmente escuchará a los propios investigadores referirse erróneamente a los datos obtenidos de una API como "extraídos". La distinción es importante, no solo por razones prácticas como ahorrar tiempo y esfuerzo, sino también por las violaciones éticas y legales que pueden derivarse de la extracción de datos de sitios web.

Considerando esta analogía básica de la diferencia entre los dos enfoques, profundicemos en los detalles de las API y la extracción de datos de sitios web.

API

Para los investigadores interesados en un enfoque más práctico para la recopilación de datos, muchas plataformas tienen una forma más directa de acceso a los datos en forma de interfaces de programación de aplicaciones (API). En términos generales, las API son una manera de que los usuarios interactúen fácilmente con un sitio web o una plataforma de redes sociales a través del código de la computadora. Esto le permite al usuario procesar rápidamente muchos más datos y, a su vez, generar información más profunda sobre la actividad en línea que lo que de otra manera podría hacer de forma manual.

6 CrowdTangle está disponible actualmente para académicos e investigadores de forma selectiva. Usted y su equipo pueden presentar su solicitud en CrowdTangle.com. La versión completa incluye datos actuales e históricos sobre Facebook e Instagram. En el sitio web también está disponible una extensión CrowdTangle gratis, la cual toma un URL como dato de entrada y ofrece las 500 publicaciones públicas más recientes que se hayan vuelto significativamente populares citando el URL en Facebook, Instagram, Reddit y Twitter. Tanto la plataforma completa como la extensión CrowdTangle pueden ser útiles para las investigaciones.

Tipos de API

En particular, hay dos características de las API que son importantes considerar antes de iniciar la recopilación de datos: la apertura y el plazo.

- **Apertura:** Las API vienen en diferentes formas; las API abiertas permiten que cualquier persona recopile datos, mientras que las API autenticadas requieren que el usuario se someta a alguna forma de verificación antes de permitirle la recopilación de datos.
  - **API abiertas:** Venmo, la aplicación utilizada para pagos electrónicos en los Estados Unidos, tiene una API pública que permite a cualquier persona ver algunas de las transacciones públicas más recientes realizadas a través de la aplicación. Puede encontrar listas de API abiertas en Internet, como esta lista en Github. Any-api.com también cuenta con una lista de varias API que están disponibles públicamente para los usuarios interesados, muchas de las cuales son abiertas.
  - **API autenticadas:** La mayoría de las API con las que trabajará para la recopilación de datos de redes sociales (Twitter, Reddit, etc.) requieren la autenticación de un usuario para poder comenzar a recopilar datos.
- **Plazo:** Los sitios web y las plataformas también suelen estructurar sus API de manera diferente dependiendo de los plazos.
  - **Recopilación de datos históricos:** La mayoría de las API permiten recopilar algún tipo de datos históricos en sus sitios: Twitter y Reddit especialmente lo permiten. Esta forma de API, llamémosla *API histórica*, permite obtener retroactivamente los datos que se generaron antes de realizar la consulta. Es importante destacar que los datos publicados después de realizar la consulta no están disponibles para su recopilación.
  - **Transmisión de datos en tiempo real:** El consumo y la descarga de datos mientras ocurre en tiempo real es un proceso denominado *transmisión en directo (streaming)*. Si Twitter es una plataforma relevante en las elecciones o el periodo que planea monitorear, es probable que la transmisión en directo sea su mejor opción para la recopilación de datos. Cuando se transmiten datos en directo, los tuits se recopilan en tiempo real según la consulta específica (por ejemplo, todos los tuits que usen la etiqueta *#elección*, o todos los tuits que mencionan cuentas de interés, o citen el URL de interés, etc.)

Limitaciones en la recopilación mediante API

En aras de preservar la privacidad y seguridad del usuario, la mayoría de las plataformas de redes sociales limitan la cantidad de datos que un usuario puede recopilar. En esta sección exploramos algunas de esas limitaciones para que se familiarice con los problemas que podría encontrar al recopilar datos.

- **Limitaciones de volumen:** La mayoría de las API limitan el volumen de datos que un usuario determinado puede recopilar. Por ejemplo, cuando se transmiten datos en directo en tiempo real en Twitter, la plataforma limita la cantidad de datos que un usuario puede recopilar al 1% de los datos de la transmisión global.
  - **Límites de velocidad:** Los límites de velocidad son el tipo más común de limitación de volumen con el que se encontrará al obtener datos mediante las API. La mayoría de las API tienen límites de velocidad para garantizar que un solo usuario o aplicación no puedan descargar una cantidad excesiva de datos (según lo defina la plataforma o el sitio web en particular). Por ejemplo, Twitter limita la cantidad de tuits que un solo usuario puede descargar en un periodo de 15 minutos.
- **Limitación de datos eliminados:** Como se mencionó anteriormente, las plataformas tienden a eliminar contenido que infringe las reglas y regulaciones de uso especificadas; estas regulaciones pueden tener distintos nombres (normas comunitarias, términos de servicio, etc.). Este hecho es particularmente importante en el caso de contextos electorales en los que es probable que ocurran comportamientos nefarios; en especial, la transmisión de datos en directo en Twitter le permite recopilar y preservar datos sobre actores nefarios en tiempo real que posteriormente podrían eliminarse de la plataforma. Una vez eliminados, los datos sobre estos actores no están disponibles. Si su equipo desea capturar actores dañinos, desinformación y demás contenido para su análisis posterior, la transmisión en directo en tiempo real maximiza sus posibilidades de hacerlo.
- **Limitaciones del tipo de datos:** Del mismo modo, la mayoría de las plataformas limitará el tipo de datos que un usuario puede recopilar de su plataforma. La API de Twitter le permitirá recopilar cierta información sobre un usuario objetivo (como el número de publicaciones, el número de seguidores y la fecha de creación de la cuenta), pero no le permitirá acceder a otros tipos de datos restringidos (como la dirección IP que un usuario utiliza con más frecuencia). Actualmente Facebook no permite que los investigadores recopilen información sobre otros usuarios o páginas a través de su API. Al diseñar un proyecto de investigación, es útil saber cuál es el tipo de datos que se pueden recopilar en las plataformas objetivo.

- **Limitaciones de tiempo de los datos:** Cuando se recopilan datos históricos a través de la API de búsqueda de Twitter, la plataforma limita el acceso de los usuarios a los datos que se hayan producido en los últimos 7 a 9 días. Los datos que tienen más de 7 a 9 días en Twitter se pueden comprar a proveedores de datos como GNIP, pero no se pueden recopilar a través del acceso estándar a la API.

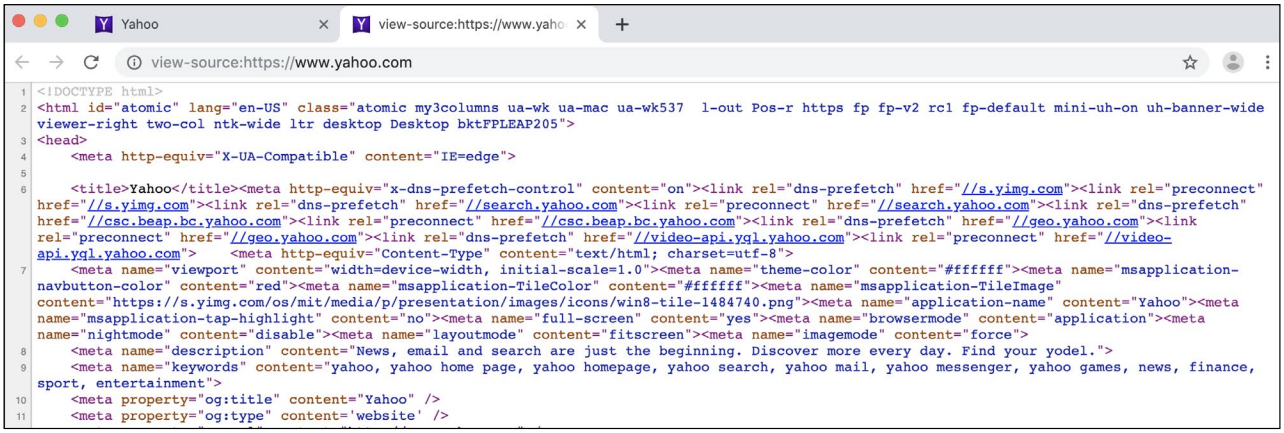
Un aspecto interesante de las API es que no tienen un lenguaje específico. Los datos de la API se pueden recopilar utilizando Java, Python, R, Ruby, Perl o cualquier otro lenguaje de programación que usted o su equipo de tecnología prefieran. Sin embargo, existen paquetes específicos en lenguajes de programación populares que simplifican el proceso de consulta de la API al encargarse por usted de algunas de las complejidades.

Al final de esta guía, en el Apéndice, está disponible un código de ejemplo con explicaciones que muestran cómo usar el paquete Rtweet de R para recopilar datos de la API de búsqueda y transmisión en directo de Twitter: *Ejemplo de código de API: Cómo recopilar datos de las API de búsqueda y transmisión en directo de Twitter con el paquete Rtweet*.

Extracción de datos de sitios web (*web scraping*)

Si bien las API ofrecen una forma simplificada de recopilar datos de una plataforma o servicio, no son la única opción para hacerlo. La *extracción de datos de sitios web* es el proceso mediante el cual se extrae el código fuente de un sitio web objetivo y se recuperan datos relevantes. Cada página en Internet es el resultado del código fuente que se conforma por HTML y otros lenguajes, secuencias de comandos, hipervínculos y fuentes de medios. Al proceso de que un navegador tome texto del código y lo convierta en una página web visual e interactiva se le conoce como *renderización*. En la mayoría de los navegadores modernos se puede ver el código fuente subyacente de cualquier página web; Google Chrome, Mozilla Firefox, Safari, Brave y Opera cuentan con esta función.

Por ejemplo, al utilizar Google Chrome, puede hacer clic con el botón derecho del *mouse* en cualquier página web que se haya cargado (o "*renderizado*") en su navegador y hacer clic en la opción "*Ver código fuente de la página*". Chrome abrirá una nueva pestaña que le mostrará los códigos HTML y CSS que se utilizan para cargar la página web que está viendo. A continuación se muestra un ejemplo de esto de yahoo.com.



Captura de pantalla de los códigos fuente HTML y CSS subyacentes de yahoo.com (instantánea tomada a principios de agosto de 2019). Google Chrome y otros navegadores modernos les permiten a los usuarios ver el código fuente de cualquier sitio web que visiten; este código fuente es lo que se recupera cuando se extraen los datos de un sitio web.

Preocupaciones éticas cuando se extraen datos de sitios web

La extracción de datos de sitios web puede ser una herramienta útil para analizar páginas de Internet. Sin embargo, debe tenerse en cuenta que la extracción de datos de sitios web es un incumplimiento de los términos de servicio de la mayoría de las plataformas de redes sociales, y puede ser fácil violar la ley cuando se extraen datos de sitios web. Por este motivo, al extraer datos de sitios web es importante considerar siempre la privacidad del usuario, los términos y condiciones relevantes y las leyes pertinentes. Siempre es importante asegurarse de que su proceso de recopilación de datos sea ético y legal. ***Por estos motivos, muchos investigadores solo recopilan datos a través de las API y eligen no extraer datos de sitios web.***

Si utiliza datos recopilados por otros equipos o herramientas (algo frecuente en muchos casos), también es fundamental que se asegure de que los datos con los que está trabajando se hayan obtenido de manera ética. Por ejemplo, si los datos se obtuvieron ilegalmente mediante la extracción de sitios web o la piratería informática (*hacking*), no es aconsejable utilizarlos para un proyecto de investigación por razones legales, éticas y políticas, ya que este tipo de proyectos pueden generar repercusiones tanto por parte de las autoridades gubernamentales como corporativas. Es importante tener en cuenta estas consideraciones antes de comenzar el análisis de los datos.

Diferencias entre las plataformas: *Tabla resumen*

	API histórica disponible	**API de transmisión directa (*streaming*) disponible**	**Herramientas de recopilación de datos de terceros**
Twitter	Sí	Sí	CrowdTangle (extensión)
Facebook	No	No	CrowdTangle
Gab	Sí, a través de Pushshift.io	No	No
Instagram	No	No	CrowdTangle
Reddit	Sí	Sí (ciertos paquetes tienen esta función, p. ej. Reddit SSE)	CrowdTangle (extensión) Pushshift.io
YouTube	Sí	No	
Telegram	Sí	No	Telethon Pushshift.io
VKontakte	Sí	No	
WhatsApp	Sí - la API de WhatsApp Business permite comunicaciones automatizadas de empresas a clientes. Por lo general no se utiliza para el tipo de análisis del que hablamos en esta guía.	No	Varias herramientas de terceros permiten el análisis estadístico o la visualización de los chats de WhatsApp[7]. ▪ ChatAnalyzer ▪ WhatsApp Chat Analyzer ▪ Chatilyzer ▪ WhatsAnalyzer

Herramientas útiles para recopilación de datos en un contexto de integridad electoral:

- **Paquetes de API de Twitter:**
  - Paquetes R: rtweet, twitteR
  - Paquetes Python: python-twitter, tweepy
- **CrowdTangle:** CrowdTangle y la extensión CrowdTangle son actualmente las mejores herramientas para analizar Facebook e Instagram.
- **Pushshift.io:** Es un sitio que archiva datos de plataformas de redes sociales (Reddit, Gab, Twitter y Telegram). El fundador y operador de Pushshift, Jason Baumgartner, obtiene sus datos mediante el acceso a las API, lo que hace que el uso de los datos sea seguro desde una perspectiva ética.
  - **Herramienta de transmisión en directo de Reddit:** https://github.com/pushshift/reddit_sse_stream

7 Es importante tener muy claras cuáles son las implicaciones de privacidad del uso de estas herramientas. En particular, cuando se encuentren con herramientas de análisis de WhatsApp, usted y su equipo deben asegurarse de que los chats privados no se expongan a ningún tercero ni que estos los guarden.

- **MIT Media Cloud:** MIT Media Cloud es una herramienta de agregación de noticias que puede ser útil para explorar la cobertura de temas de interés en diversos medios. Al describir la herramienta, el sitio web dice *"Agregamos datos de más de 50,000 fuentes de noticias de todo el mundo y en más de 20 idiomas, incluyendo español, francés, hindi, chino y japonés. Nuestras herramientas ayudan a analizar, entregar y visualizar información sobre conversaciones de medios en tres niveles principales: picos de atención y cobertura de problemas, análisis de redes y uso de lenguaje agrupado"*.

Análisis de datos y redes

La construcción de representaciones visuales de redes sociales y el análisis de las relaciones internas es un proceso que se conoce como análisis de redes sociales (ARS). También se refieren comúnmente a este proceso como construcción de un mapa de redes sociales o "mapeo" de redes sociales. Si bien no siempre es necesario utilizar el análisis de redes sociales para comprender el ámbito de los medios en línea en torno a una elección, puede ser una manera útil de generar ideas informativas sobre la influencia dentro de una franja determinada de una comunidad de redes sociales, y puede ser eficaz para visualizar esa comunidad.

En esencia, hacer un mapa de las redes sociales es un proceso que consta de 5 pasos:

1. Recopilación de datos
2. Decisión sobre qué relación mapear
3. Poda de datos
4. Generación del mapa
5. Análisis del mapa

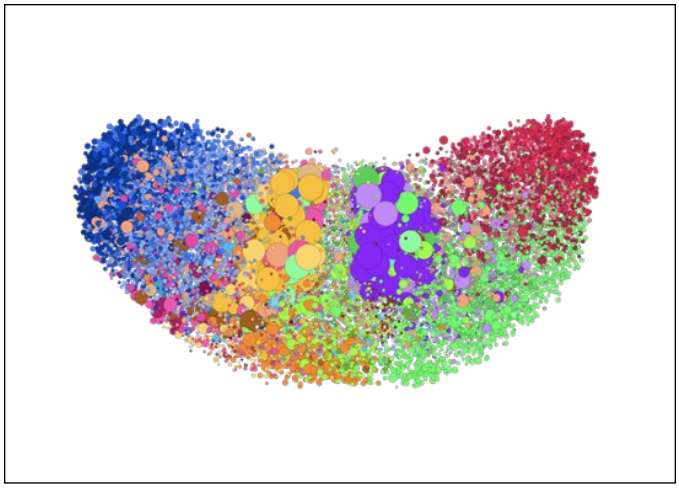
A continuación se analizará cada uno de estos pasos en mayor detalle.

Terminología básica

Cuando se revisan y analizan mapas de redes sociales, hay algunos términos que son útiles para ayudar a entender el vocabulario y las prácticas típicas del monitoreo de redes sociales. Las redes son extremadamente útiles porque pueden representar muchas relaciones en varios contextos diferentes. Si bien los mapas de redes sociales son probablemente los más conocidos, las redes se pueden usar para modelar la propagación de enfermedades y virus, mapear la actividad neuronal en el cerebro o representar posibles rutas para viajar de una ciudad a otra. Aunque esta aplicabilidad de las redes a tantas áreas distintas es útil, también crea la necesidad de contar con un lenguaje abstracto para hablar de redes, independientemente del campo de aplicación, por lo cual, en esta sección se presentan brevemente algunos términos básicos que le serán útiles en este aspecto.

Los más relevantes *son grafo, nodo* y *arista*.

- **Grafo:** En computación, *grafo* es el término para referirse a una red que se compone de *nodos y aristas*. Es importante conocer esta palabra, ya que puede encontrarla en herramientas que hacen mapas de redes o en conversaciones sobre esas herramientas. En términos generales se puede considerar que la palabra *grafo* es sinónimo de *red*.
- **Nodo (o vértice):** Los *nodos* son los elementos que conforman una red. Algo muy importante que debe saber acerca de los nodos es que lo que representa un nodo puede variar dependiendo del mapa o la visualización que esté analizando. En el mapa de redes de los sitios web a favor del Kremlin elaborado por Lawrence Alexander, un nodo representa un dominio, mientras que cada nodo circular en el mapa de Graphika del panorama político estadounidense en 2018 en Twitter, representa una cuenta de Twitter.



Este mapa de Graphika del espectro político de los Estados Unidos en 2018 en Twitter ilustra los nodos. Cada círculo en el mapa es un nodo que representa una cuenta individual de Twitter. Los nodos y las aristas son los dos componentes básicos de las redes.

- **Arista (o arco):** Las aristas son las conexiones entre los nodos de una red, representados más comúnmente como una simple línea entre dos nodos. Estas conexiones pueden representar varias cosas. En un modelo de contagio de enfermedades, las aristas pueden representar la propagación del virus de un huésped a otro. En un grafo de aeropuertos en los Estados Unidos, las aristas entre dos nodos (aeropuertos) pueden representar un vuelo directo disponible entre ambos aeropuertos. Las aristas pueden ser dirigidas o no dirigidas[8], y pueden tener un valor numérico asociado con ellas[9] (a menudo denominado *peso*).
    - Es probable que las aristas de los grafos de las redes sociales representen una de las siguientes cosas: relaciones de seguimiento, retweets, o "me gusta". La mayoría de las redes que vemos en Twitter serán *redes de seguidores*[10] (en las que la *arista* muestra que un usuario sigue a otro), o *redes de retuiteo*.

Cómo hacer un mapa de redes sociales: pasos a seguir

En esta sección definiremos y analizaremos los cinco pasos a seguir en la creación de un mapa de redes sociales a partir del cual se generará información.

1. **Recopilación de datos:** Como se vio en la sección anterior, este paso implica la recopilación de datos relevantes para una elección local a través de una API de redes sociales o una herramienta de terceros. Una vez que se recopilan los datos, se tiene el conjunto de datos base que necesitará para hacer una visualización de las redes sociales. Es importante considerar *que solo se usarán partes de estos datos en la generación del mapa*; el mismo conjunto de datos base se puede usar para generar todo tipo de mapas. En los pasos 2 y 3 hablaremos de cómo elegir qué tipo de red o relaciones le interesan más y qué datos son más relevantes.
2. **Decisión sobre qué relación mapear:** En el mapa de su red social, es probable que cada "nodo" (es decir, cada círculo en el mapa) represente una cuenta de Twitter o una página de Facebook. Sin embargo, las *relaciones* entre estos nodos (relaciones de "me gusta", relaciones de seguimiento, retuits, etc.) son las que le dan su estructura a la red de nodos relevantes. En otras palabras, esta relación es la que determina el esqueleto del mapa, y a partir de ese esqueleto se extraen relaciones relevantes acerca de los nodos en el mapa. En la teoría de grafos (el campo de la informática que se ocupa de las redes y el mapeo), estas conexiones también se conocen como *aristas*.

8 Por ejemplo, el grafo que modela el contagio viral del ejemplo anterior puede tener una dirección asociada con la propagación de la infección, en este caso, la arista se movería del que infecta al infectado, y se representaría con una flecha.

9 En el ejemplo anterior del grafo del aeropuerto, los valores de las aristas podrían ser la distancia en kilómetros entre los aeropuertos. Otro posible valor de la arista para este grafo sería el tiempo que lleva volar de un aeropuerto a otro.

10 Para ver ejemplos de redes de seguidores, vea aquí una red de cuentas que promueven mensajes contra las vacunas en Wired.

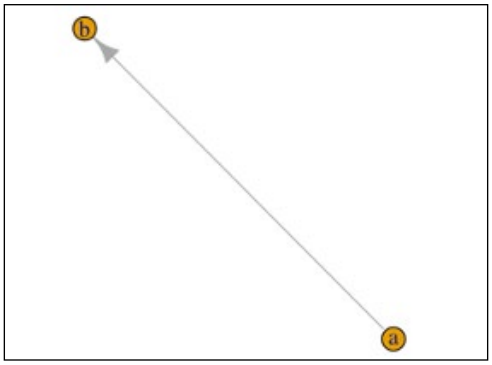
3. **Poda de datos:** Si recopila una gran cantidad de datos, casi siempre terminará con más de los que puede mapear. Affinio, NodeXL, Gephi y otras herramientas de generación de mapas tienden a funcionar mejor en el rango de unos cuantos miles de nodos. El mapeo a una mayor escala generalmente es demasiado costoso desde el punto de vista computacional para ser útil; por esta razón, es necesario determinar cuál es la red más relevante para sus preguntas. En computación, al proceso de eliminar datos superfluos a menudo se le denomina *poda*; también es probable que escuche otros términos, como *reducción de redes o reducción de dimensionalidad*. Algunas herramientas (por ejemplo, Graphika) hacen este trabajo de reducción de redes por usted, pero también hay herramientas, como Gephi, que le permiten tomar decisiones sobre los umbrales. Algunos ejemplos pueden ser mapear solo nodos que han usado una etiqueta (*hashtag*) relacionada con las elecciones más de una vez, o solo incluir nodos que tengan una conexión con cinco o más nodos en la red.[11]
4. **Generación de mapas:** Una vez que decida qué relación mapear (aristas) y qué nodos estarán en su red mediante la reducción de redes, estará listo(a) para hacer su mapa. Generalmente en esta etapa tendrá que poner sus datos relevantes en un formato que sea legible para la herramienta que está utilizando (por ejemplo, un archivo *CSV*, un archivo graph.graphml o un archivo *.gexf* para Gephi), y hacer que su software lo lea. Después de esto, la mayor parte del trabajo duro se hará por usted. Hay muchos tutoriales gratuitos y útiles en YouTube sobre generación de mapas de redes con Gephi[12] y otras herramientas de código abierto.
5. **Análisis de mapas:** Una vez que se genere su mapa, puede personalizar las imágenes y pasar al análisis. Normalmente, las medidas de *centralidad* son clave para entender la influencia en una red. *Analyzing Social Networks* [Análisis de las redes sociales] (Borgatti, Everett y Johnson 2019) tiene un capítulo completo dedicado a los distintos tipos de centralidad que vale la pena consultar.[13]

Ejemplos de tipos de redes

Como se mencionó anteriormente, hay varios tipos de redes que pueden generarse a partir de un determinado conjunto de datos. El factor clave determinante para saber qué tipo de red está mapeando radica en la *relación* que ha elegido mapear. En Twitter existen dos tipos comunes de redes dirigidas que se utilizan con frecuencia para analizar datos: redes de seguidores y redes de retuiteo. Ambos tipos de redes pueden ser útiles para analizar datos e influencia.

Redes de seguidores

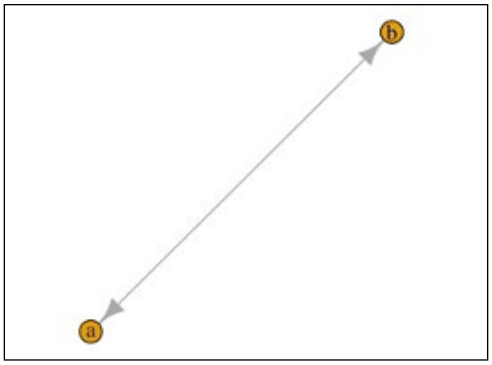
En una "red de seguidores", los nodos son cuentas de Twitter y las conexiones entre ellos representan las relaciones de seguimiento. Normalmente estas conexiones son direccionales (provienen de un nodo a otro en una dirección particular). Se podría decir que son líneas que significan "*sigue*". Por ejemplo, el siguiente grafo muestra dos nodos, A y B, y muestra que "A *sigue* a B".



Representación de una relación de seguimiento unidireccional: en este diagrama, A sigue a B. Esto se representa mediante una sola línea dirigida (o flecha) de A a B.

Observe que en este grafo solo hay una relación de seguimiento en una dirección, es decir, A sigue a B, pero B *no* sigue a A. Si hubiera una relación de seguimiento mutua, en la que A y B se siguieran entre sí, la representación de la red mostraría flechas en ambos sentidos, como en la siguiente figura.

11 Este tipo de poda se conoce como *reducción del k-núcleo*.
12 Gephi también ofrece un tutorial gratuito en PDF y otros materiales de aprendizaje en su sitio oficial: gephi.org.
13 Capítulo 10, *Centrality*. Este libro es un excelente texto para aprender los conceptos básicos sobre redes y métodos de análisis de redes. Como siempre, también puede encontrar en línea todo tipo de excelentes tutoriales gratuitos y de fuentes abiertas.



Representación de una relación de seguimiento mutua: A sigue a B y B sigue a A.

En las redes generadas a partir de los datos de Twitter en torno a una elección, es probable que tenga muchos más de dos nodos en su red relevante. Los ejemplos anteriores sirven para darle una idea de los componentes básicos con base en los cuales se construye una red compleja.

Ventajas y desventajas de las redes de seguidores

Las relaciones de seguimiento, en especial en Twitter, son de cierto modo relaciones permanentes y de largo plazo, ya que los usuarios no suelen dejar de seguir a otros usuarios. Por esta razón, las redes de seguidores representan una visión a más largo plazo de la dinámica de las redes y los flujos de información que las redes de retuiteo. Por otro lado, los usuarios tienden a tener más de un interés en Twitter; esto abre la posibilidad de que algunos de los usuarios de su red de seguidores quizás no sean tan relevantes como le gustaría para el contenido que le interesa. Las redes automatizadas a menudo tienen enfoques más monotemáticos, por ejemplo, para apoyar a un partido, candidato(a) o cuestión en particular, pero aun así, con frecuencia varían en contenido. Sin duda, es un aspecto a considerar cuando se analizan las cuentas para buscar automatización u otras formas de actividad coordinada.

Sería completamente posible, por ejemplo, que en un mapa hipotético del espectro político estadounidense se tenga una franja de la red que tuiteó principalmente sobre cultura y música pop, pero que estaba significativamente conectada a una red de cuentas principalmente políticas. Es útil tener en cuenta estas ventajas y desventajas al decidir si una red de seguidores es de interés o no para su investigación.

Redes de retuiteo

Las redes de retuiteo son otro tipo de relación en Twitter; en estas redes, las conexiones entre los nodos representan *quién retuiteó a quién* dentro de los datos recopilados. En este sentido, estos mapas están más orientados al contenido que las redes de seguidores. A continuación se muestra una representación de las aristas dentro de este tipo de grafos.

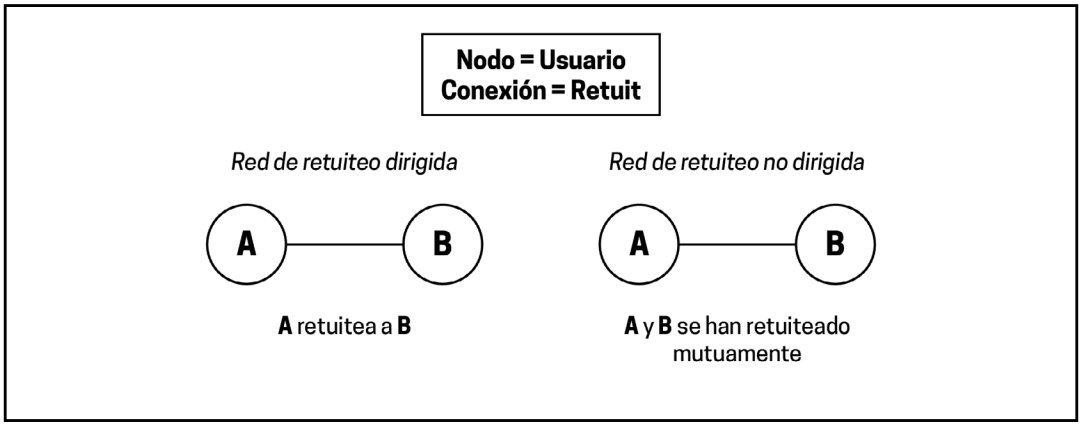
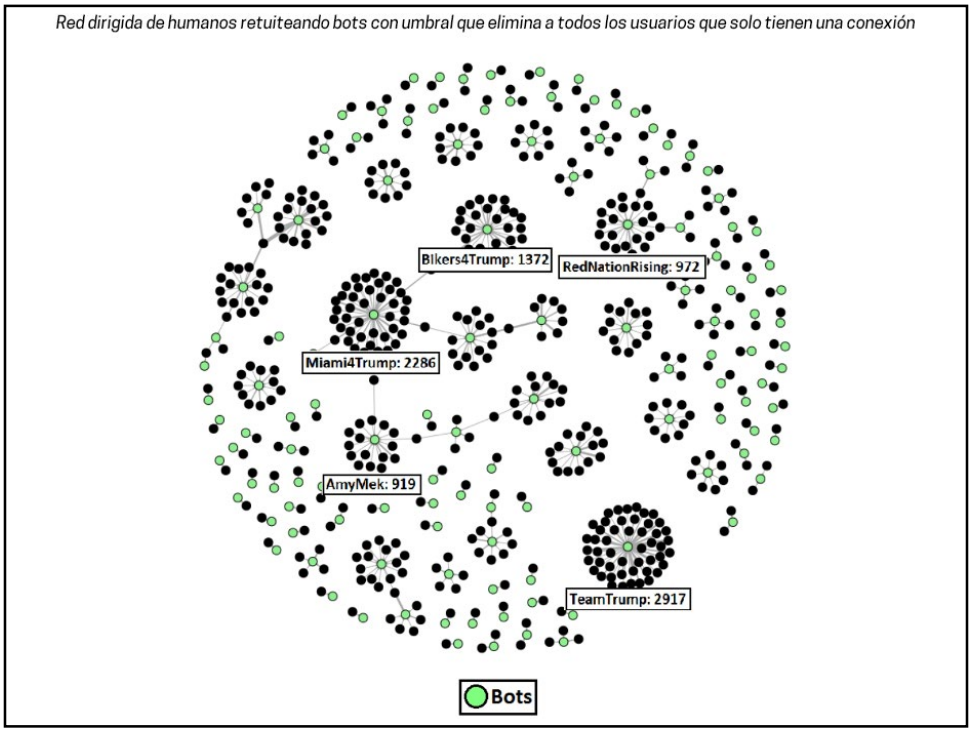


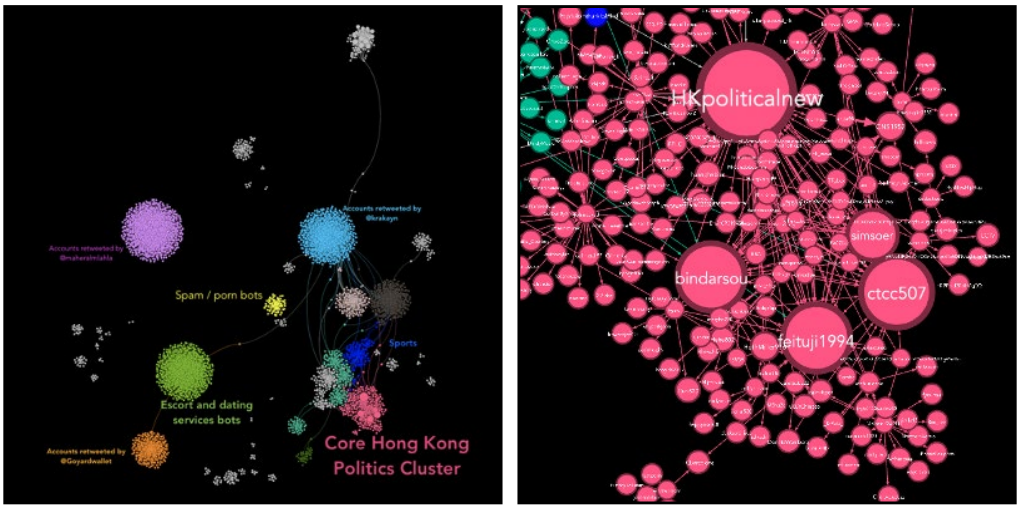
Diagrama que representa nodos y aristas dentro de una red de retuiteo. (Fuente: Samuel Woolley y Douglas Guilbeault (2017). Computational Propaganda in the United States: Manufacturing Consensus Online. Disponible aquí.)

Ventajas y desventajas de las redes de retuiteo

Estas redes son un tanto más efímeras que las redes de seguidores, ya que las redes de retuiteo representan una instantánea en el tiempo: quién retuiteó a quién en un periodo determinado. En este sentido, son una descripción precisa de la dinámica de influencia en un periodo corto, como una campaña de etiquetas (*hashtags*) dedicada o los días anteriores a una elección.



Red de retuiteo generada a partir de datos de Twitter recopilados en torno a las elecciones presidenciales de Estados Unidos en 2016. En esta red, los nodos que representan las cuentas de bots son verdes y las cuentas humanas son negras, y al observar los retuits entre los usuarios, vemos que los humanos retuitearon de manera significativa el contenido de los bots en las elecciones presidenciales de 2016. (Fuente: Samuel Woolley y Douglas Guilbeault (2017). Computational Propaganda in the United States: Manufacturing Consensus Online. *Disponible aquí.)*

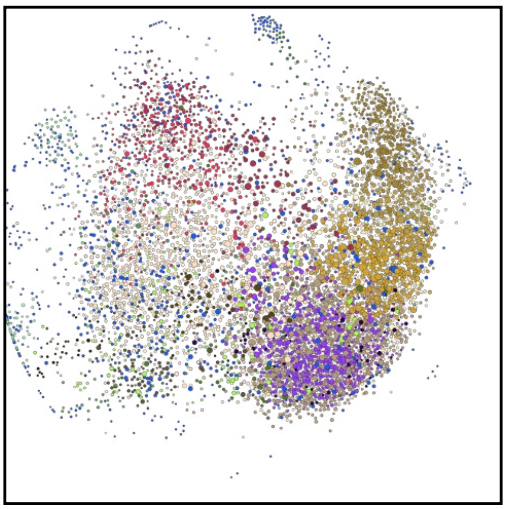


Imágenes de una red de retuiteo de cuentas del gobierno chino difundiendo información para desacreditar las protestas en favor de la democracia en Hong Kong de junio a agosto de 2019. Esta red de retuiteo se compiló a partir del archivo de operaciones de información de Twitter[14]. Estas imágenes representan la red de retuiteo completa (izquierda) y una vista ampliada del principal grupo político dirigido a Hong Kong (derecha). (Fuente: Informe del Laboratorio de Inteligencia Digital del Instituto para el Futuro, disponible aquí.)

14 Específicamente desde el lanzamiento de tuits atribuidos al gobierno chino en agosto de 2019.

Redes de menciones

Los mapas de menciones son otro tipo común de mapa con el que es probable que se encuentre. La idea es muy parecida a la de los mapas de retuiteo (las aristas representan "menciones") en los que un usuario menciona a otro. Mediante el uso de datos de Gab reunidos por Pushshift.io, Graphika generó un mapa de una red de menciones para analizar conversaciones y comunidades en la plataforma social Gab, una red social que es muy similar a Twitter en cuanto a su uso y construcción.



Mapa de menciones de Graphika sobre usuarios de Gab. Este mapa se compiló a partir del conjunto de datos de Gab disponible públicamente en Pushshift.io, el cual abarca desde agosto de 2016 hasta finales de octubre de 2018.

Las redes de seguidores, retuiteo y menciones son solo algunas de las opciones que tiene para generar redes a partir de datos de Twitter, pero ciertamente existen otras posibilidades. En otras plataformas, como Facebook o Gab, es posible que existan otras relaciones. Por ejemplo, podríamos imaginar un mapa de red de páginas públicas y relaciones de "me gusta".

Limitaciones de la recopilación de datos y el mapeo de redes

Como ocurre con cualquier herramienta, el mapeo de redes tiene ciertas limitaciones al igual que el proceso de recopilación de datos que lo precede. Las dos limitaciones más importantes a considerar son la *escala* y el *tiempo*. Como se mencionó en la sección de recopilación de datos, todas las herramientas disponibles para generar mapas de redes, ya sean gratuitas o de paga, actualmente tienen limitaciones de escala. Esto se debe a que a medida que aumenta el número de nodos en una red, el número de conexiones posibles aumenta *exponencialmente*[15]. Esta cantidad de datos es agobiante, incluso para las computadoras, y por lo tanto es poco probable que encuentre una herramienta que pueda generar un mapa de más de 15,000 nodos[16]. Sin embargo, sería un error ver esta limitación exclusivamente como un problema: una parte importante de la ciencia de datos y el análisis de datos implica elegir qué partes de un gran conjunto de datos tienen más probabilidades de producir información útil. Dicho de otra manera, analizar los datos adecuadamente implica elegir qué partes de los datos vale más la pena investigar; en este sentido, la ciencia de datos es tanto un arte como una ciencia. Esta tarea, la cual es una parte central de la investigación, el análisis y el entendimiento de los datos, no siempre se facilita al tener más datos.

La segunda limitación que probablemente encuentre con respecto a la recopilación de datos y el mapeo de redes es una limitación de tiempo, específicamente cuando se recopilan datos históricos. La API estándar de búsqueda de Twitter solo permite la recopilación de datos históricos desde una semana previa al momento de la consulta. Los datos que tengan más de 7 a 9 días deben provenir de otra fuente, como una herramienta (de paga) que permita una recopilación histórica más amplia o la compra de datos a un proveedor de datos, como GNIP. Si bien el análisis de datos históricos puede ser útil en ciertos casos, la compra de datos históricos puede volverse costoso rápidamente. Por esta razón, **la mejor solución es siempre recopilar todos los datos relevantes en tiempo real**. Si usted o algún miembro de su equipo está interesado en transmitir en directo o recopilar datos en torno a una elección, siempre es mejor comenzar a recopilar tan pronto como tenga una idea clara de lo que le interesará.

15 Para aquellas personas interesadas en las matemáticas, una red de *n* nodos tiene *n*(n-1)/2* posibles conexiones.

16 El software de mapeo de Graphika actualmente puede mapear a la mayor escala, permitiendo la visualización de hasta 5.5 millones de nodos

Redes cerradas y cifradas

Un desafío al que se enfrentan los esfuerzos de monitoreo de medios en los últimos años es la popularidad y la adopción generalizada de aplicaciones de mensajería cifrada como WhatsApp, Telegram y Signal. Cada vez más, los medios en los que los ciudadanos confían para mantenerse al tanto de los acontecimientos políticos durante las elecciones y demás eventos políticos importantes ocurren en estas plataformas. Países como Brasil, India y México han visto un marcado aumento en los mensajes políticos en WhatsApp, por ejemplo. Si bien el uso de redes de mensajería cifrada representa indudablemente una ventaja para la privacidad, la seguridad y los derechos digitales de la ciudadanía, también plantea nuevos desafíos para entender la difusión de la información política en línea.

En la actualidad, los mejores métodos para los esfuerzos de monitoreo de medios de redes cerradas se basan en la verificación manual de datos: equipos de expertos que monitorean los canales relevantes de WhatsApp, ya sea individualmente o en grupo, verifican las historias y distribuyen públicamente los resultados de estos trabajos. Tales esfuerzos han tenido éxito en varios casos, como el detector de WhatsApp, La Silla Vacía[17], en Colombia, así como el trabajo de Verificado[18] en México y el Centro para la Democracia y el Desarrollo en Nigeria.[19]

Otro esfuerzo notable es el del bot de Cofacts, en Taiwán. Johnson Liang y un equipo de desarrolladores que trabajan con el movimiento g0v idearon una manera de combinar la verificación manual de datos y la distribución automatizada para ayudar a la ciudadanía taiwanesa a verificar si una historia es falsa o no. Los usuarios pueden agregar el bot de Cofacts[20] en LINE, una popular aplicación de mensajería cifrada utilizada en Taiwán y Japón. Si un usuario ve una historia sospechosa, puede pegar el enlace en un chat y enviarlo al bot de Cofacts. Si la historia no se había visto antes, un equipo de personas verifica la historia y sube a una base de datos central un mensaje que resume la veracidad de la historia. Luego, el bot reenvía este mensaje al usuario original y a cualquier otro usuario que tenga curiosidad por saber si la historia es verdadera o no. Cofacts permite el acceso público de los datos anónimos que ha recopilado en Github, y también permite a los usuarios realizar búsquedas en esta base de datos a través de un sitio web público. Meedan, una compañía que apoya la verificación de hechos y otras investigaciones en línea, también ha lanzado un conjunto de herramientas similares en Check que ayudan a varios usuarios a automatizar y administrar colectivamente los flujos de trabajo para el proceso de verificación de hechos en WhatsApp y otras plataformas.

Existen ciertas herramientas, como Backup WhatsApp Chats, que permiten a los usuarios exportar conversaciones de WhatsApp a archivos CSV, pero el usuario debe pertenecer a un canal para exportar los chats desde la aplicación. Telegram, una aplicación de mensajería cifrada, tiene una API que permite a los usuarios acceder a canales públicos mediante programación. Esto permite llevar a cabo cierto grado de monitoreo de los medios públicos, aunque los datos no son tan ricos como en Twitter.

Herramientas y paquetes útiles de visualización de redes

La siguiente tabla enumera varias herramientas y paquetes de códigos populares que se utilizan para la visualización y el análisis de redes.

Herramientas de visualización y análisis de redes			
Herramientas de código abierto o gratuitas	**Herramientas de paga**	**Paquetes de uso común (Python)**	**Paquetes de uso común (R)**
Gephi NodeXL	Graphika Affinio	networkx matplotlib igraph	igraph plotrix

17 https://www.niemanlab.org/2017/03/to-slow-the-spread-of-false-stories-on-whatsapp-this-colombian-news-site-is-enlisting-its-own-readers/
18 https://www.niemanlab.org/2018/06/whatsapp-is-a-black-box-for-fake-news-verificado-2018-is-making-real-progress-fixing-that/
19 https://www.cddwestafrica.org/whatsapp-nigeria-2019-press-release/
20 El nombre chino de este bot es 真的假的, que significa "verdadero o falso".

Identificación de *influencers*, grupos y cuentas

El objetivo de recopilar y analizar datos es entender la manera en que se distribuye la información dentro de una red. ¿Qué historias están ganando fuerza? ¿Qué usuarios son los más influyentes? ¿Qué dominios de noticias se citan con más frecuencia en la conversación? Con un sólido conjunto de datos y las herramientas adecuadas, puede comenzar a responder estas preguntas con especificidad y deducir la dinámica de la difusión de información en el espacio en línea que está observando.

Existen dos formas de conceptualizar la influencia en las redes sociales: estos métodos para identificar la influencia pueden ser *basados en contenido y basados en actores*. A continuación analizaremos ambos métodos.

Métodos para identificar la influencia basados en el contenido

Los métodos basados en contenido se centran en tuits, etiquetas (*hashtags*), palabras clave o sitios web en forma de URL o dominios.[21] En algunos escenarios, se conocerá a los actores que vale la pena observar: por ejemplo, medios o políticos que a menudo difunden desinformación. Por otro lado, es bastante común no conocer las fuentes de desinformación, discursos de odio u otras formas de contenido que se están buscando.

A menudo, este método puede ser más útil cuando se analizan conversaciones en línea sobre elecciones u otro discurso político a fin de entender qué contenido está ganando más fuerza, especialmente cuando no se está buscando analizar a un actor en particular que se haya identificado en los datos. Observar qué URL o tuits se están volviendo populares en los datos puede ser un buen lugar para comenzar en este escenario.

Tuits

Cuando se analizan los tuits, se puede estimar la influencia al observar la cantidad de retuiteos o "me gusta" que han conseguido[22]. Ya sea que utilice una herramienta de terceros u obtenga datos de la API de Twitter, debe tener fácil acceso a estos datos en todo momento. Después de determinar qué tuits son los más influyentes, puede usar ese tuit como trampolín para llevar a cabo una investigación más amplia. Algunas de las preguntas que vale la pena investigar son:

- ¿Quién creó originalmente el tuit? ¿Quién ha retuiteado la publicación? ¿Qué tan grande es el número de seguidores de estos usuarios? Si es grande, es posible que valga la pena realizar un análisis de redes sobre ellos.
- ¿Qué etiquetas (*hashtags*) se usan en el tuit? Si alguna de ellas es muy característica o solo la promueve un pequeño grupo de usuarios, ¿hay algo que estos usuarios tengan en común?
- ¿Qué URL están presentes en la publicación? Si el URL es sospechoso (se creó recientemente o promueve la desinformación), es posible que valga la pena investigar un poco más, como por ejemplo, verificar los datos de registro del dominio a través de una consulta en Whois[23] o buscar en Twitter otras menciones interesantes del URL. También puede utilizar la extensión del navegador CrowdTangle para ver si este URL se está volviendo popular en Facebook, Instagram, Reddit o en cualquier otro lugar de Twitter.

Estas mismas estrategias y principios también son válidos para Facebook, Twitter, Gab y otras plataformas de redes sociales: analizar las interacciones con una publicación es una forma confiable de medir la influencia de un mensaje en una determinada comunidad.

Etiquetas (*hashtags*) y palabras clave

Las etiquetas son naturalmente una de las principales entidades de interés cuando se analizan datos de Twitter y de otras redes sociales. La convención de usar una etiqueta para destacar el tema de lo que se está tuiteando es una bendición para los investigadores: nos permite recopilar con gran facilidad los datos de conversaciones relevantes sobre un tema de interés. Una vez que se ha identificado una etiqueta o conjunto de etiquetas de interés, existen varias posibilidades para una investigación

21 Los URL se refieren a un enlace completo que lo lleva a una historia o sitio en particular, mientras que los dominios se refieren al sitio que aloja ese contenido; esto corresponde al texto que precede al dominio de nivel superior (abreviado como TLD, como *.org, .com, .gov*, etc.) y el propio TLD. Por ejemplo, los tres URL example-news-site.com/story1, example-news-site.com/story2 y example-news-site.com/story3 están alojados en el mismo dominio: *example-news-site.com*.

22 Un dato interesante que se debe tener en cuenta con respecto a los tuits es que estos tienden a tener más "me gusta" que los retuiteos. Esto se asemeja al hecho de que la mayoría de las publicaciones de Facebook tienen más "me gusta" que "compartir". Si estas proporciones son anormales, puede ser un indicador de actividad no auténtica, aunque de ninguna manera es una garantía.

23 Existen muchas bases de datos de Whois para verificar los detalles de registro, una de ellas, que es confiable, es la que tiene la Corporación de Internet para Nombres y Números Asignados (ICANN, por sus siglas en inglés) https://lookup.icann.org/.

más profunda; algunas opciones son analizar las etiquetas que más comúnmente ocurren al mismo tiempo, dividir las citas de la etiqueta por tiempo o analizar los URL simultáneos.

URL y dominios

Los localizadores de recursos uniformes (URL, por sus siglas en inglés) y los dominios que aparecen dentro de los tuits, los cuales a menudo se enlazan a fuentes de noticias, son una fuente extremadamente útil para determinar qué contenido, publicaciones y narrativas están ganando más fuerza dentro de una determinada comunidad en línea.

Un primer paso común en el análisis de los URL o dominios es extraer URL únicos de un conjunto de datos y contar la cantidad de veces que se citan dentro del conjunto. Esta técnica es sencilla y poderosa, pero también es fácil equivocarse de varias maneras sutiles, pero significativas. Para garantizar que su análisis arroje la información más precisa y útil, le recomendamos prestar atención a las cuestiones que se indican a continuación.

- **Expansión de URL acortados** - Los URL en tuits a menudo se acortan para que quepan dentro de los límites de caracteres; el uso de una herramienta de expansión de URL le dará el URL completo que el URL acortado indica. Ciertas herramientas, como URLex.org, ofrecen una API para la expansión masiva y automatizada de URL. Esta es la mejor manera de asegurarse de que no le falten datos en los URL acortados.
- **Estandarización de URL** - Se puede citar el mismo dominio utilizando diferentes cadenas de texto[24]. Por ejemplo, los enlaces al *New York Times* pueden aparecer en el texto como www.nytimes.com, nytimes.com, NYTimes.com, http://nytimes.com, nyti.ms, https://nytimes.com, http://www.nytimes.com, https://www.nytimes.com, o m.nytimes.com (estas son solo algunas de las posibilidades). A fin de garantizar que no se subestime la influencia de un URL o dominio al contar diferentes cadenas, es recomendable asegurarse de estandarizar el formato antes de contar. No siempre será posible controlar todas las distintas formas en que los URL que llevan al mismo contenido pueden aparecer, pero considerar la estandarización con anticipación puede ser de gran ayuda para mejorar sus análisis. Los aspectos que tienen que tomarse en cuenta al estandarizar son (1) mayúsculas y minúsculas[25], (2) prefijos (http://, https://, www., ww2., etc.) y (3) subdominios, entre otros factores.

Después de analizar los URL más populares de un conjunto, existen varias opciones para llevar a cabo un análisis más detallado. Si el dominio es una fuente de noticias relativamente nueva en la escena, puede usar técnicas de inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés) como verificar la información de registro del dominio para comenzar a obtener información sobre las conexiones del dominio. Las OSINT son una forma útil de recopilar más información sobre cuentas o sitios web de interés. Es un campo que cambia constantemente, en el que las herramientas y técnicas aparecen y desaparecen todos los días. Una de las mejores fuentes para aprender nuevas habilidades es Intel Techniques, pero existen muchas otras. Bellingcat, un colectivo de investigadores que a menudo documenta las operaciones de influencia rusas, ha creado una forma artística de utilizar las OSINT para producir historias periodísticas innovadoras, y mantiene un documento público de Google[26] con un inventario exhaustivo de herramientas de investigación y OSINT. Lawrence Alexander, un científico de datos con sede en el Reino Unido, utilizó astutamente los códigos de Google Analytics para realizar un mapa de una red de sitios web a favor del Kremlin en 2015.

Después de deducir cuáles son los sitios web y artículos más influyentes de un conjunto de datos dado, también puede hacer un análisis de contenido para analizar qué narrativas ocurren en esos artículos. Las técnicas de PNL (procesamiento del lenguaje natural), como el uso de frecuencias de n-gramas para analizar las frases más comunes en esos artículos, las frecuencias de término-frecuencias inversas de documentos (tf-idf, por sus siglas en inglés) para comparar los temas relativos de distintos artículos, o el uso de métodos de análisis cualitativo de contenido pueden conducir a resultados informativos una vez que haya limitado el conjunto a algunos artículos y URL influyentes.

24 En un contexto computacional, los datos de texto a menudo se denominan "*cadenas*". Esto es para acortar el nombre completo: *cadenas de caracteres*, y así es como los científicos informáticos a menudo se refieren al texto de los tuits o publicaciones en los conjuntos de datos de redes sociales.
25 La distinción entre mayúsculas y minúsculas se refiere a si los datos de texto están escritos con minúsculas o con mayúsculas. Estos problemas se manejan más fácilmente si todos los URL del conjunto se escriben en minúsculas antes de contar el número de ocurrencias de cada URL. Sin embargo, es importante tener en cuenta que, si bien la mayoría de los URL completos no distinguen entre mayúsculas y minúsculas, muchos de los URL acortados sí lo hacen. Por lo tanto, se recomienda que los investigadores resuelvan primero la expansión del URL antes de pasar a estandarizar o escribir el URL en minúsculas.
26 https://docs.google.com/document/u/1/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit

Métodos basados en la red

Otra forma de analizar la influencia en un conjunto de datos es adoptar un enfoque basado en la red. En este enfoque, se utilizan los datos para construir una red relevante tal como se mencionó en la sección anterior *Análisis de datos y redes*; estos podrían ser menciones, seguidores, retuiteos u otras métricas basadas en la red.

Creación de clústeres o grupos

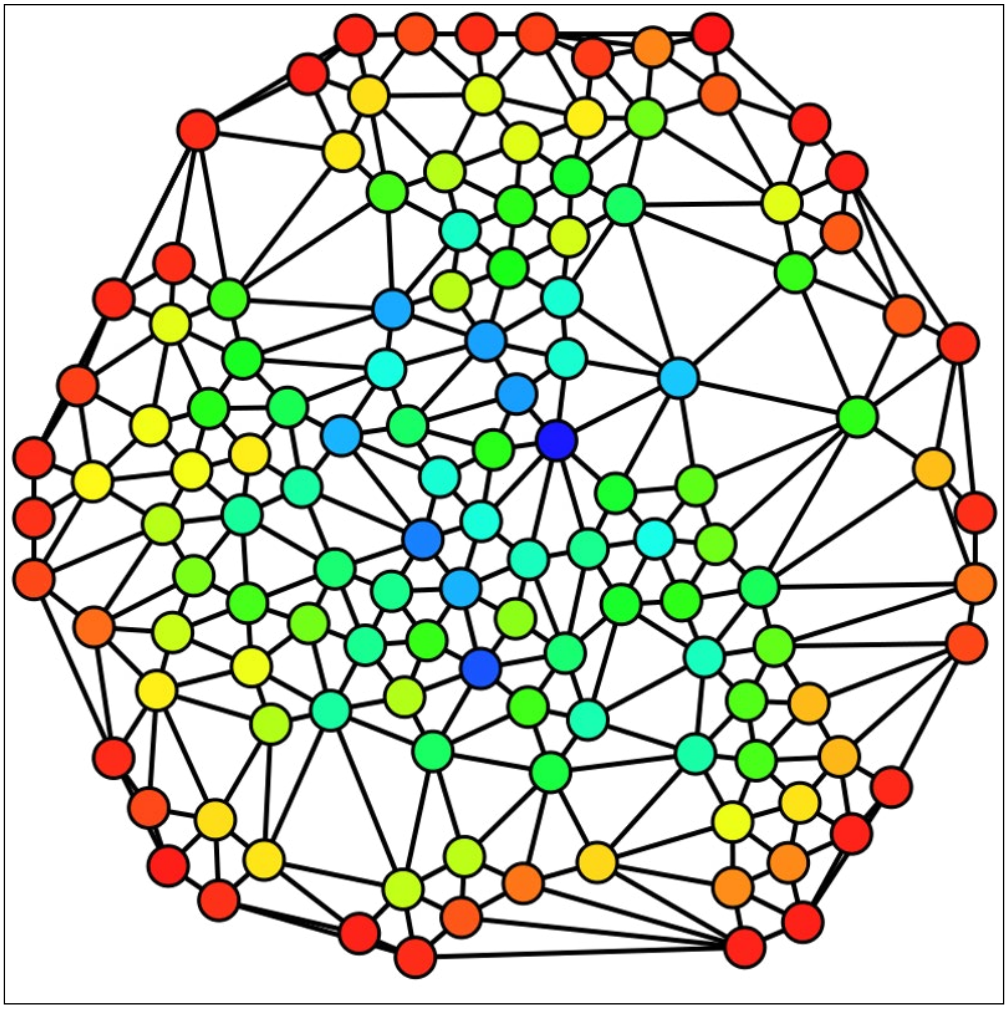
La detección de comunidades es la base del trabajo más significativo que compara comunidades (a menudo denominadas *clústeres* en el ARS). Si bien existen complejas teorías metodológicas que sustentan diferentes algoritmos para la creación de clústeres, la mayor parte del trabajo pesado lo realizará el software que utilice. Gephi ofrece varias opciones para el diseño y la creación de clústeres de la comunidad (puede encontrar más detalles en el tutorial aquí). Graphika también hace este trabajo automáticamente. Basta decir que una vez que su software de visualización y análisis de redes determina el número de comunidades diferentes en su red, puede pasar al análisis cualitativo para determinar qué tienen en común los miembros de un clúster determinado.

A menudo, las comunidades y los clústeres de cuentas tendrán características distintivas en común, como promover fuentes de noticias similares o pertenecer a un partido semejante. Aquí es donde la comprensión del contexto político general se vuelve importante. La combinación del análisis cuantitativo de los datos de la comunidad con el análisis cualitativo del contenido es la mejor manera de determinar qué tienen en común los miembros de una comunidad dada.

Centralidad

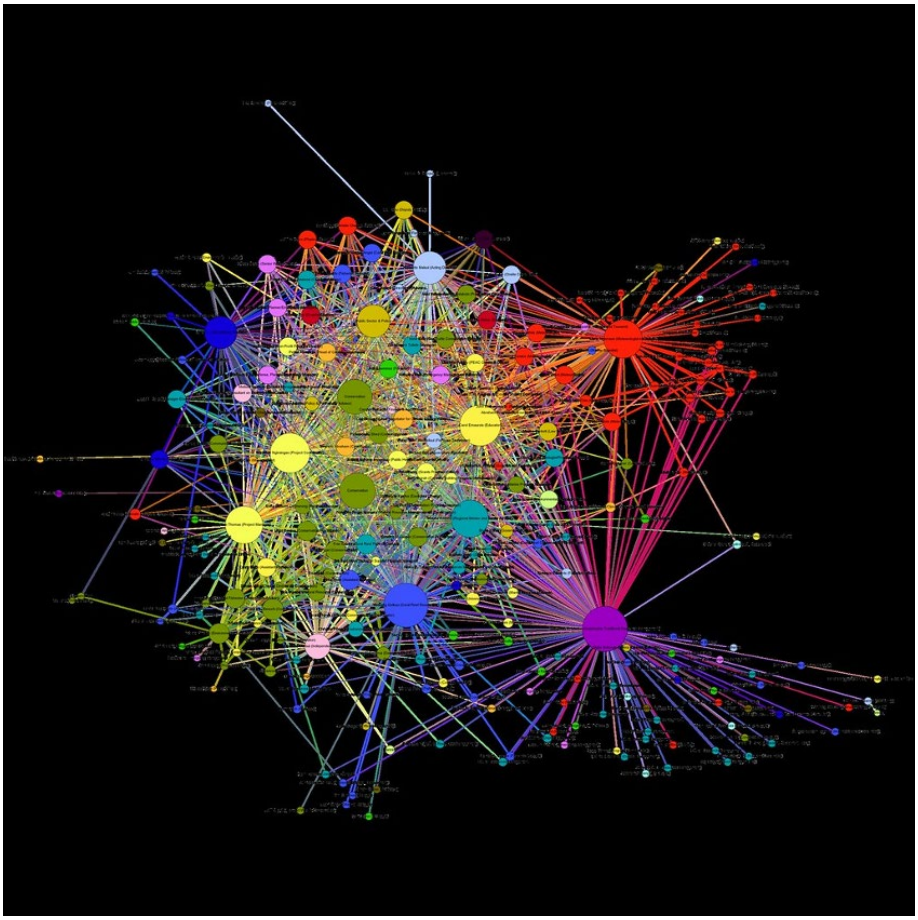
En la teoría de redes, específicamente cómo se aplica al ARS, la métrica principal para analizar la influencia de un solo actor o grupo de actores es la *centralidad*. La centralidad mide qué tan bien conectado está un nodo dado o cuán influyente es este dentro de una red. Existen varios métodos diferentes para medir la centralidad.

- **Centralidad de grado:** En un grafo no dirigido, la centralidad de grado de un nodo dado es el número de conexiones directas que tiene con otros nodos a su alrededor. En un grafo dirigido, donde se tiene en cuenta la dirección de la arista, hay dos tipos de centralidad de grado: *centralidad en grado*, o cuántas conexiones entrantes tiene un nodo, *y centralidad fuera de grado*, o cuántas conexiones salientes tiene un nodo. En estos escenarios, la centralidad en grado es posiblemente la más relevante: un nodo con un gran número de conexiones entrantes tiene un alto potencial de influencia. Este es un concepto relativamente intuitivo: una cuenta con 15,000 seguidores (un grado entrante de 15,000) tiene una mayor capacidad de influir directamente que una cuenta con 100 seguidores. La importancia de la centralidad en grado o fuera de grado varía según la red que se esté analizando.
- **Centralidad de intermediación:** Se puede considerar que la centralidad de intermediación mide la capacidad de un nodo para difundir un mensaje a otros nodos rápidamente. Dicho de otra manera, la centralidad de intermediación otorga puntuaciones más altas a los nodos que probablemente sean vectores para viralizar o diseminar mensajes más rápidamente. Este valor se mide contando el número de veces que un nodo determinado se encuentra como parte de la ruta más corta de un nodo a otro.



La tonalidad (de rojo = 0 a azul = máximo) indica la centralidad de intermediación de cada nodo. (Claudio Rocchini) Creative Commons BY 2.5 https://en.wikipedia.org/wiki/Social_network_analysis#/media/File:Graph_betweenness.svg

- **Centralidad de vector propio:** La centralidad de vector propio es muy útil para comprender la influencia dentro de una determinada red o subred. La idea detrás de la centralidad de vector propio es esencialmente: "¿quién influye en los *influencers*?". Con la centralidad de vector propio, la influencia depende menos del número de vínculos que un nodo objetivo tiene con otros nodos, y más de cuántas conexiones tiene el nodo objetivo con otros nodos bien conectados. Se podría decir que esta versión de centralidad es como un tipo de "influencia de goteo": ¿qué tan probable es que la información que fluye desde un nodo fuente se propague a otros nodos influyentes? El motor de búsqueda de Google utiliza una forma de este concepto, ya que clasifica las páginas (o nodos) de acuerdo con la cantidad de otras páginas que hacen referencia a ellas. Los nodos con una alta centralidad de vector propio pueden desempeñar un papel particularmente poderoso en la diseminación de bienes (como dinero, información, gérmenes, etc.) a través de una red.



Proyecto de análisis de redes sociales de Pacific RISA, mapa centrado en Palau; todos los miembros son o están conectados a Palau. Los nodos se ordenan según la centralidad de vector propio y se colorean según la profesión. *Creative Commons BY 2.5* *https://www.flickr.com/photos/pacificrisa/11344578486*

- **Puentes:** Aunque no es una forma de centralidad, los *puentes* son un fenómeno útil de la estructura de las redes que se debe considerar. Un nodo o un pequeño conjunto de nodos actúan como un *puente* cuando conectan un clúster denso con otro clúster denso. Sin puentes, los clústeres de distintos intereses (como los miembros de dos partidos políticos independientes, o los aficionados políticos en dos países diferentes) no tendrían medios para transmitir información o comunicación entre ellos. En este sentido, los puentes son partes importantes del contenido viral en las redes en línea.
- **Hojas:** Las *hojas* son nodos en un grafo con una sola arista que los conecta a una red. A menudo vale la pena eliminar estas cuentas de una red, especialmente redes grandes, en las que es muy poco probable que tengan alguna influencia.

Existen disponibles en línea varios tutoriales y recursos útiles sobre los diferentes tipos de centralidad; un recurso útil es el libro *Analyzing Social Networks* [Análisis de las redes sociales] (Borgatti et al., 2013), cuyo capítulo 10 presenta diferentes tipos de centralidad y la manera en que se miden.

Las herramientas de código abierto como Gephi pueden hacer por usted el difícil trabajo de calcular en segundos[27] las distintas formas de centralidad. En última instancia, la decisión de qué forma de centralidad utilizar es responsabilidad de usted y su equipo. Si bien consultar a un científico de datos o a un teórico de redes es ideal para tomar esta decisión, en este caso, no es necesario que se preocupe demasiado por las minucias metodológicas: casi todas las formas de centralidad suponen que los nodos más influyentes son, en cierto sentido, los nodos con el mayor número de vínculos en una red o subred.

Una vez que haya determinado qué forma de centralidad le interesará usar, puede incluso personalizar las imágenes de su red para reflejar esto. Gephi le permite, por ejemplo, utilizar el tamaño del nodo o tonos de color para resaltar la centralidad.

27 O minutos, dependiendo de qué tan grande sea la red en cuestión.

Cómo identificar fuentes de noticias

En el caso del análisis de las elecciones y de la información en particular, la cuestión de cuántas fuentes de noticias se citan en los datos es de fundamental importancia. Esta es un área en la que es especialmente útil trabajar con personas que tengan un profundo entendimiento social y político del país o la región en cuestión. Las fuentes de noticias que se citan con más frecuencia son a menudo ya conocidas para estas personas. Como se mencionó anteriormente, es importante tener un sólido entendimiento del entorno de medios subyacente en el país, incluyendo la participación en el mercado y la influencia de la televisión, la radio, los periódicos y los medios en línea.

Existen varios métodos útiles para identificar nuevas fuentes de noticias en una región o conjunto de datos. Una opción es realizar búsquedas manuales frecuentes en Google de noticias y política de la región, especialmente en varios idiomas si la región es multilingüe. Es probable que las fuentes de noticias que compiten por la influencia tengan una sólida optimización de los motores de búsqueda (SEO, por sus siglas en inglés) para mostrarlas dentro de los primeros resultados retenidos por Google, y a menudo pueden mostrar fuentes de noticias creadas recientemente de las cuales el ciudadano promedio no está enterado. Otra opción, que es muy recomendable, es llevar a cabo un análisis de las veces que se citan los dominios y los URL en un conjunto de datos. Esto puede hacerse de varias maneras: monitoreando CrowdTangle para ver los principales URL en un conjunto determinado de páginas políticas, o extrayendo los URL o dominios únicos de los datos publicados[28] en un conjunto de datos recopilados con un experto local y buscar dominios que ninguno de ustedes haya visto antes. Crowdtangle tiene un complemento gratuito para Chrome y otros navegadores que le permite ver las veces que se ha compartido un artículo en particular, pero para acceder a su tablero y otras herramientas más avanzadas, los usuarios deben obtener una licencia institucional, a menudo a través de Facebook, que es la actual empresa propietaria.

La idea principal aquí es que, a menudo, la desinformación emana de dominios recién creados que aparecen rápidamente en torno a cuestiones políticas y elecciones, y desaparecen con la misma rapidez. Este fue el caso de *streetnews[.]one*, un dominio que fue creado y promovido en Gab en el periodo previo a las elecciones intermedias de los Estados Unidos en 2018. El dominio se usó para difundir contenido islamofóbico y sensacionalista antes de que desapareciera rápidamente. Este fue también el caso en Endless Mayfly, un análisis de la desinformación iraní realizado por el Laboratorio Ciudadano de la Universidad de Toronto junto con expertos de la industria. En este caso, el equipo del Laboratorio Ciudadano acuñó la frase, "*desinformación efímera*", para describir los dominios de desinformación que aparecen y desaparecen rápidamente y que se enfocan en temas clave, elecciones y campañas.

El uso de listas de dominios de desinformación o sitios web de noticias falsas en esta etapa puede ser extremadamente útil. Un grupo de investigadores de Stanford elaboró una lista de más de 600 dominios conocidos por producir contenido falso a fines de 2018, dirigidos principalmente a los Estados Unidos (Allcott *et al*, 2018)[29]. Si alguna vez decide usar tales listas, deben tomar en cuenta dos advertencias importantes: (1) la desinformación y el espacio en línea se mueven rápidamente: los nuevos dominios de desinformación que se han producido desde que se compiló la lista, no estarán incluidos en el análisis; y (2) cualquier lista utilizada debe ser revisada y aprobada adecuadamente mediante rigor metodológico: el uso de listas elaboradas al azar que se encuentran en línea podría ser perjudicial para la integridad de la investigación.

Análisis de cuentas y contenido

Una vez que haya recopilado datos y/o creado una red de cuentas relevantes que le interesen, usted y su equipo estarán listos para comenzar a analizar las cuentas y el contenido del conjunto de datos. Es probable que esta sea la parte del trabajo en la que pasará la mayor parte del tiempo, especialmente si inicialmente no sabe lo que está buscando.

El análisis de contenido se realiza mejor si se oscila entre métodos cualitativos y cuantitativos, a menudo repitiendo el proceso varias veces para encontrar cuentas específicas o contenido de interés. En esta sección le daremos algunos consejos y herramientas para ayudarle a llevar a cabo este trabajo.

28 De preferencia, junto con las veces que se citan, cuenta como una estimación de la popularidad de estas fuentes. Otros métodos, como la extracción de los URL de las publicaciones más retuiteadas o con más "me gusta" en un conjunto de datos, también son formas de estimar la influencia de un dominio en particular dentro de un conjunto de datos.

29 Puede encontrar este artículo aquí.

Tipos de contenido

Antes de sumergirse de lleno en los datos, es útil tener una idea de algunos de los tipos de contenido que le sugerimos buscar en el conjunto de datos.

- **Desinformación e información errónea:** El contenido político falso y engañoso es una de las formas más dañinas de contenido que deberá detectar en su conjunto de datos. Aunque al contenido falso se le puede llamar de distintas maneras, incluyendo propaganda computacional y noticias falsas, a este tipo de contenido se le conoce comúnmente como desinformación o información errónea. La diferencia técnica entre estos dos términos radica en la intención detrás del contenido falso[30]. Las definiciones que usaremos para diferenciar estas dos palabras están tomadas del informe *Lexicon of Lies* [Léxico de mentiras] de Data and Society (Jack 2017), el cual explora un conjunto de palabras que son útiles para entender y usarse cuando se habla de contenido falso en línea.
  - **Desinformación:** Contenido falso que se difunde con la intención deliberada de engañar. Los actores estado-nación motivados políticamente o los actores motivados económicamente son los actores que más probablemente distribuirán intencionalmente la desinformación, según se define esta.
  - **Información errónea:** Información falsa que, sin saberlo, se difunde y distribuye. Si una cuenta promueve una historia sin tener la intención de engañar a los usuarios, esto califica como información errónea.
  - **Mala información:** Algunos autores también han destacado el fenómeno de la "mala información": la distribución de información verdadera o mayormente veraz con la intención de causar daño. Claire Wardle y Hossein Derakhshan definen la mala información como "*Información que se basa en la realidad, utilizada para infligir daño a una persona, organización o país*" (Wardle y Derakhshan 2017).
- **Discurso de odio:** El discurso de odio es un lenguaje que demoniza a las personas de una raza, etnia, género, orientación sexual o religión objetivo. A menudo, el discurso de odio incita a otros a acosar, denigrar o incluso participar en la violencia contra el grupo social objetivo.

Análisis lingüístico

Una manera de analizar el contenido de forma rigurosa es llevar a cabo un análisis lingüístico, el cual puede ayudarle a entender cuáles son los principales idiomas de los mensajes, los principales temas de contenido, las narrativas que se promueven y desarrollan, las nuevas palabras clave y la jerga, y si en la conversación se produce el discurso de odio o algún otro contenido peligroso.

Palabras clave y léxicos

Es probable que no todas las publicaciones o tuits de un determinado conjunto de datos sean significativos para las preguntas específicas que le interesan a usted. Por tal motivo, puede ser útil compilar una lista de palabras clave relevantes que probablemente contengan información pertinente para su consulta. Trabajar con un experto en la materia, alguien que tenga un profundo entendimiento del idioma y la política de la región de interés, es la mejor manera de garantizar la calidad de una lista de palabras clave. En ocasiones, estas listas de palabras clave también se denominan "léxicos" si todas se relacionan con un tema común. Por ejemplo, a menudo se utilizan léxicos del discurso de odio en diferentes idiomas que se relacionan con distintos contextos políticos para analizar el contenido político. Incluso una sesión rápida de una hora con un experto en la materia puede contribuir en gran medida a introducir cierto rigor en la compilación de listas de palabras clave para garantizar su calidad. También puede consultar literatura académica relevante y usar listas de palabras clave compiladas previamente si son de alta calidad y pertinentes para su contexto.

Ejemplos de léxicos

Existen numerosos ejemplos de léxicos que están disponibles en línea y son útiles para el análisis lingüístico y la extracción de publicaciones relevantes. El equipo de Género, Mujeres y Democracia del NDI compiló un léxico del discurso de odio relacionado con los idiomas indonesio, keniano y serbio (Zeiter et al., 2019). PeaceTech Lab, una organización sin fines de lucro dedicada al uso de tecnología para promover la paz en países en vías de desarrollo, también tiene varios léxicos del discurso de odio disponibles públicamente de forma gratuita en su sitio web. Estos léxicos son multilingües, lo que puede ser extremadamente útil para monitorear conversaciones en varios lugares o en regiones con alta diversidad lingüística.

30 Si bien este es el caso, a menudo no es posible conocer la intención detrás del contenido falso que se propaga en línea. Por esta razón, es probable que a veces escuche estas palabras usadas indistintamente.

Hatebase.org también tiene listas multilingües de palabras clave del discurso de odio. Los académicos Roya Pakzad y Nilhoufar Salehi utilizaron una lista compilada de este sitio web para su estudio de propaganda computacional dirigida a los musulmanes estadounidenses en las elecciones intermedias de 2018 en los Estados Unidos (2019). Una lista similar se utilizó para realizar un análisis cuantitativo de la islamofobia en Gab en el periodo previo a las mismas elecciones (Woolley, Pakzad y Mónaco, 2019).

Análisis lingüístico cualitativo

Una vez que haya extraído un conjunto relevante de publicaciones, puede meterse de lleno en el análisis lingüístico. Los métodos cualitativos son aquellos que analizan el contenido y los temas de los mensajes de las publicaciones en su conjunto de datos. Este tipo de trabajo es más eficaz cuando lo realizan personas (en lugar de máquinas) y lo lleva a cabo un experto o equipo de expertos que estén familiarizados con el contexto político y lingüístico de la región en cuestión.

Ya sea que utilice métodos cualitativos, cuantitativos o ambos durante su análisis, es muy importante que sus métodos sean consistentes y sistemáticos. Utilizar los mismos métodos para analizar cada publicación o parte de su conjunto de datos es la mejor manera de evitar introducir sesgos en sus resultados.

Análisis narrativo

El análisis narrativo es una forma intensiva de analizar el contenido lingüístico en un conjunto de datos, pero puede ser muy interesante. El análisis narrativo que examina la manera en que ciertos medios se refieren a un tema determinado, especialmente a lo largo del tiempo, puede darnos una idea sobre el planteamiento y la influencia de los medios en la opinión pública.

Codificación cualitativa

Otro método cualitativo que es útil para entender qué tipos de mensajes están ocurriendo en un determinado conjunto de datos es el que se conoce como *codificación* cualitativa. Esto consiste en que un equipo de expertos, de manera independiente, le asignen a cada una de las publicaciones una categoría tomada de un conjunto de categorías (o "códigos") predefinidas. Después de asignar categorías a cada tuit, se puede llevar a cabo un análisis cuantitativo.

Por ejemplo, en un estudio hipotético sobre una elección presidencial entre dos candidatos, el candidato A y el candidato B, en el país imaginario de Qumar[31], podemos imaginar cinco posibles categorías para los mensajes recopilados en torno a las elecciones:

1. Pro candidato(a) A
2. Pro candidato(a) B
3. Anti candidato(a) A
4. Anti candidato(a) B
5. Neutral

Una vez que el equipo de expertos ha codificado todas las publicaciones del conjunto de datos, existen varios análisis cuantitativos que podríamos realizar como siguiente paso:

- **Distribución de publicaciones en cada categoría:** Podríamos analizar la cantidad de publicaciones que aparecen en cada categoría para examinar si hubo un mayor apoyo u oposición en línea para el candidato A o el candidato B.
- **Uso de palabras clave por categoría:** También podríamos analizar las publicaciones de cada categoría en busca de palabras clave relevantes, a fin de ver si los partidarios o la oposición de cualquiera de los candidatos utilizan ciertas palabras.
- **Contenido de bots en cada categoría:** Otra posibilidad es revisar las publicaciones de cada categoría en busca de contenido de robots informáticos (bots) para ver si el candidato está obteniendo un mayor apoyo u oposición de agentes automatizados en línea.

Estos son solo algunos ejemplos del análisis que se puede llevar a cabo después de realizar una codificación cualitativa de alta calidad.

31 Qumar es un país ficticio que aparece en la serie de drama político estadounidense *The West Wing*.

Análisis lingüístico cuantitativo

El análisis lingüístico cuantitativo también se conoce como procesamiento del lenguaje natural (PNL) o lingüística computacional. Los métodos utilizados en el análisis lingüístico cuantitativo surgen de la idea de que podemos obtener algunos conocimientos sobre los tipos y las frecuencias de ciertos mensajes cuando vemos el lenguaje desde un punto de vista estadístico. Dicho de manera más concreta, si agregamos palabras o conjuntos de palabras provenientes de publicaciones relevantes de nuestro conjunto de datos, podemos analizar qué tipos de temas surgen. Esta subsección le presentará algunos de los conceptos básicos para extraer conteos de palabras de un conjunto de datos para analizar temas comunes en línea.

Si bien las técnicas presentadas en esta sección se pueden implementar con cualquier lenguaje de programación, vale la pena señalar que Python y R vienen con varios paquetes que simplifican el proceso. Estos paquetes, como el kit de herramientas de lenguaje natural de Python (NLTK) o el paquete tm de R (tm, por sus siglas en inglés, que significan *extracción de texto*) tienen una amplia documentación en libros, guías en línea y tutoriales que pueden enseñarle los conceptos básicos en unas pocas horas. Le recomendamos ampliamente que se tome un tiempo para familiarizarse con alguno de estos paquetes, especialmente si ya conoce un poco de Python o R. ¡Unas cuantas horas adicionales con anticipación, le ahorrarán mucho tiempo a usted y a su equipo!

N-gramas

Los *n-gramas* son la base de casi todos los análisis lingüísticos cuantitativos del contenido de las redes sociales. Un *n-grama* es una secuencia de palabras de longitud *n*. En particular, los siguientes tres tipos de n-gramas son los más comunes para el análisis lingüístico cuantitativo de textos:

- **Unigramas:** Una sola palabra también puede considerarse como una secuencia de 1 palabra. Este tipo de n-grama se conoce como *unigrama*.
- **Bigramas:** Un par de palabras que aparecen *una al lado de la otra* en una oración forman un bigrama. Dicho de otra forma, un bigrama es cualquier secuencia de dos palabras que aparece en un texto.
- **Trigramas:** A estas alturas, probablemente ya adivinó que un trigrama es cualquier trío de palabras que aparece en una oración. Cada secuencia de tres palabras dentro de una sola oración o texto forma un trigrama.

Es más común trabajar con estos tres tipos de n-gramas, debido en gran parte al hecho de que el uso de valores más grandes para n es "computacionalmente costoso": es probable que disminuya el rendimiento de su computadora y no obtenga muchos resultados a cambio. En el caso de secuencias con más de tres palabras, lo más común es referirse a estas simplemente con el número en cuestión seguido de la palabra "-grama". Por ejemplo, 4-gramas sería una secuencia de cuatro palabras, 5-gramas sería una secuencia de cinco palabras, etc.

La idea principal detrás de los n-gramas es que no solo nos da el conteo de palabras, sino que también tiene algo del *contexto* en el que se encuentra una palabra. Saber que la palabra "rey" aparece 16 veces, nos dice que estamos frente a un tema frecuente, pero no mucho más que eso. Si ampliamos el análisis a 4-gramas y observamos que la frase "que muera el rey" aparece 15 veces, y la frase "larga vida al rey" aparece una sola vez, podemos decir con certeza que la mayoría de las publicaciones relacionadas con el "rey" en su conjunto de datos no son mensajes de apoyo.

Una vez que su equipo se sienta cómodo con la técnica de extraer n-gramas y contar las frecuencias de los n-gramas dentro de un texto, puede aplicar esta técnica a diferentes partes de su conjunto de datos. Por ejemplo, comparar n-gramas entre cuentas o páginas que admiten diferentes candidatos(as) o partidos políticos, puede ser esclarecedor. Comparar las frecuencias de los n-gramas de distintos medios de comunicación que producen artículos relevantes para la misma elección nos puede dar una idea del enfoque principal de cada uno de los medios. Las comparaciones de la frecuencia de los n-gramas entre las historias publicadas en dos cuentas o páginas distintas pueden dilucidar los temas favoritos de sus mensajes. Estos son solo algunos ejemplos de las opciones que podrían ayudar a mejorar su investigación.

Otras técnicas lingüísticas cuantitativas

Reunir las frecuencias de los n-gramas es una técnica que se puede aplicar como el primer paso para otras técnicas de PNL que pueden ayudar a analizar un conjunto de datos con mayor detalle. Por ejemplo, después de extraer las frecuencias de palabras o de n-gramas, se puede utilizar una técnica estadística conocida como *frecuencia de término-frecuencia inversa de documento* (tf-idf, por sus siglas en inglés) para comparar entre sí los temas de los mensajes de distintos documentos. Estos "documentos" pueden ser, por ejemplo, colecciones de artículos de diferentes medios de noticias en el periodo previo a las

elecciones o historias publicadas en distintas cuentas de interés. La técnica Tf-idf es una forma básica de determinar qué temas únicos distinguen un documento de otro y podría utilizarse para analizar qué cuentas promueven con mayor frecuencia a un partido determinado, o qué distingue los mensajes de una comunidad de todos los demás que se están analizando.

Puede encontrar una introducción rápida sobre cómo usar tf-idf para el análisis lingüístico[32] y la creación de clústeres de contenido en *Mining the Social Web* (Russell y Klassen 2018). Vale la pena consultar este documento, el cual incluye un código de ejemplo en Python y es especialmente fácil de leer.

Detección automatizada de discursos de odio

Para analizar el discurso de odio en un conjunto de datos, lo más probable es que primero tenga que compilar una lista de términos sensibles del discurso de odio que sean relevantes para la región que está analizando. Estos términos deben revisarse en detalle con un experto en la materia y en todos los idiomas que podrían usarse en la región en cuestión, metodología que se describe en el informe del NDI "*Tweets That Chill*". (Zeiter et al., 2019)

Una técnica heurística para la detección automática del discurso de odio sin recurrir a la compilación de palabras clave es utilizar la API Perspective, de Google Jigsaw, una herramienta de código abierto que se introdujo en 2017. La API Perspective actualmente solo ofrece soporte para comentarios en inglés[33]. Toma una cadena de texto como entrada y genera un puntaje de toxicidad para ese texto. Cuanto más alto es el puntaje, más "tóxico" es el enunciado según los modelos de aprendizaje automático de la API Perspective. En el conjunto de datos Gab, de Pushshift.io, puede encontrar un ejemplo del uso de esta API. Además de contener publicaciones de Gab, Pushshift.io analizó cada publicación mediante la API Perspective y registró el puntaje de toxicidad obtenido.

Actualmente la API Perspective es una de las pocas herramientas disponibles públicamente que asigna puntajes de toxicidad al idioma. Se necesita mucho tiempo y esfuerzo para capturar los matices del contexto y la intención en el lenguaje humano, y por esta razón, el análisis de sentimientos y las herramientas de detección del discurso de odio todavía están en pañales. Además de la inherente dificultad general del problema, la variada especificidad del contexto de cada idioma y del contexto social en el que ocurre el discurso de odio agrava la dificultad de producir herramientas automatizadas de detección del discurso de odio que sean rigurosas y confiables. Por estas razones, trabajar en colaboración con expertos en la materia para reunir palabras clave y léxicos relevantes sigue siendo el mejor método para analizar el discurso de odio dentro de un conjunto de datos de redes sociales.

Robots informáticos (bots)

Mucho se ha escrito sobre la influencia de los bots en las redes sociales en los últimos años. El Proyecto de Propaganda Computacional (ComProp) de la Universidad de Washington y el Instituto de Internet de Oxford (OII, por sus siglas en inglés) hicieron un trabajo pionero sobre los bots, al explorar su influencia en la difusión y promoción de la propaganda computacional en países de todo el mundo.

En pocas palabras, los bots son programas de cómputo que controlan perfiles en sitios de redes sociales, a menudo haciéndose pasar por personas reales e interactuando con otros humanos en línea. En el caso de las redes sociales, la mayoría de los bots se controlan a través de programas de cómputo que controlan las cuentas mediante la API[34]. Los más sencillos de estos bots a menudo tienen signos reveladores que delatan que están automatizados, por ejemplo, tuitean en el mismo minuto de cada hora o no tienen una foto de perfil. Estos datos a menudo se usan en algoritmos de aprendizaje automático para herramientas que distinguen a los bots de los humanos en línea.

---

32 Este texto también le presentará algunas técnicas relevantes para mejorar su análisis, como la eliminación de palabras vacías y la lematización (*stemming*).

33 Durante los siglos XX y XXI, el inglés se ha beneficiado de manera desproporcionada de la atención de los lingüistas, tanto computacionales como no computacionales. Los idiomas que no se han beneficiado de una gran atención e investigación a menudo se denominan *idiomas de bajos recursos* en lingüística y PNL. No se puede sobreestimar la importancia de producir investigación en estos idiomas. Si usted o su equipo llevan a cabo una investigación lingüística o del discurso de odio como parte de sus esfuerzos de monitoreo de los medios, sería recomendable que se comunique con lingüistas profesionales en la industria o la academia para ver si su investigación podría ayudar a aportar información valiosa en el campo.

34 En la sección anterior sobre recopilación de datos, exploramos las diferencias entre las API y la extracción de datos de sitios web: esta diferencia también es útil para entender la manera en que operan ciertos bots en las redes sociales y en la web en general sin el uso de las API. Los bots se pueden programar para interactuar con páginas web cotidianas; de hecho, esto es algo bastante trivial para los programadores. Por ejemplo, los bots pueden ir de un sitio a otro y analizar el contenido de las páginas web; este tipo de bots a menudo se llaman *rastreadores o arañas*, y de hecho, así es como Google recopila datos en páginas web para poner en sus motores de búsqueda. Del mismo modo que no todos los bots son bots de redes sociales, no todos los bots son malos, y de hecho, algunos de ellos son necesarios para que el Internet funcione todos los días tal como lo conocemos.

Herramientas para detectar bots

Si bien a menudo no hay una manera segura de decir con certeza si una cuenta es un bot o no, existen opciones útiles disponibles para que el investigador curioso detecte bots en línea. Actualmente, una de las mejores opciones disponibles es Botometer, una herramienta que utiliza el aprendizaje automático para asignar a las cuentas entrantes un puntaje de probabilidad de que sean bots. Detrás de Botometer hay una larga historia de investigación y desarrollo académico en la Universidad de Indiana y es de uso gratuito. También existen otros clasificadores (consulte la siguiente tabla).

Herramientas para detectar bots

Nombre de la herramienta	¿Se puede implementar a través del código para la clasificación de lotes de cuentas?	Plataforma[35]	¿Extensiones / sitio web disponibles?
Botometer	Sí (Phython)	Twitter	Las cuentas individuales se pueden verificar en el sitio web
Tweetbotornot	Sí (R)	Twitter	Disponible solo la implementación de código
Botcheck.me	No	Twitter	Extensión de Chrome
Botsentinel	No	Twitter	Aplicación de Android y extensión de Chrome o Firefox
Pegabot	No	Twitter	Sitio web

35 Las herramientas de código abierto para detección de bots solo se han desarrollado en Twitter, en gran parte porque la API de Twitter ofrece un amplio conjunto de información sobre los usuarios (metadatos públicos), los cuales son útiles como características en la construcción de modelos de aprendizaje automático que clasifican las cuentas como de bots o de humanos. El análisis de la actividad de los bots en otras plataformas depende en gran medida del análisis y la investigación manuales, como detectar actividad sobrehumana (100 publicaciones por minuto, publicación de mensajes en intervalos regulares, etc.). Por ejemplo, en un estudio de islamofobia previo a las elecciones intermedias de los Estados Unidos en 2018 en la plataforma de redes sociales Gab, detectamos la presencia de un bot de desinformación al analizar publicaciones idénticas que ocurrían en intervalos cortos que se originaban de un solo usuario.

Conclusiones

En última instancia, todas estas técnicas y herramientas deberían ayudar a formar el enfoque del usuario para la recopilación y el análisis de datos. Asimismo, los usuarios también deberían considerar crear un flujo de trabajo utilizando estas técnicas, un sistema para archivar y clasificar la información recopilada, y potencialmente enviarla a las plataformas u otras agencias nacionales que puedan actuar con base en los datos recopilados. Dependiendo del tema, se deben considerar varias de las distintas herramientas y técnicas descritas anteriormente. Ya sea que se busque desinformación durante una elección o discursos de odio y propaganda computacional en el discurso político tradicional en línea, estos recursos se pueden aplicar de diferentes maneras. A medida que desarrollen su proyecto, los equipos e investigadores también deben considerar los recursos que tienen, tanto humanos como financieros y técnicos.

Muchas de las herramientas mencionadas son de código abierto, pero otras son costosas y a menudo complejas y difíciles de aplicar si no se tiene un conocimiento sofisticado de las herramientas y los métodos involucrados en su desarrollo. Por lo general, vale la pena considerar soluciones más sencillas que los investigadores menos experimentados puedan aplicar, o bien, trabajar en colaboración con equipos que posean diferentes habilidades para descubrir distintos tipos de información en el mismo conjunto de datos. Considere crear alianzas entre investigadores locales y expertos técnicos internacionales con el fin de obtener nuevos tipos de información, y trabajar para desarrollar métodos de colaboración en línea entre comunidades, países y regiones.

Una forma de encontrar socios con quienes colaborar en su contexto local e internacional y vincularse con empresas de redes sociales para informar e investigar es a través de la Coalición Design 4 Democracy. La Coalición D4D es un grupo de ONG internacionales que incluyen el NDI, el Instituto Republicano Internacional, la Fundación Internacional para Sistemas Electorales, IDEA Internacional y organizaciones nacionales de la sociedad civil de todo el mundo que colaboran con compañías tecnológicas como Facebook, Microsoft y Twitter para alentarlos a diseñar sistemas, moderación de contenido y políticas en favor de los principios democráticos. La investigación y el monitoreo en línea se han convertido en componentes cruciales de las elecciones y las democracias en todo el mundo, y esta guía está escrita con el fin de dar a los grupos que trabajan para apoyar estas ideas a través de políticas y sistemas técnicos, las herramientas, los métodos y las capacidades para hacer este trabajo y ayudar a informar mejor a la sociedad.

A continuación se presentan algunos recursos donde podrá obtener más referencias, herramientas de código abierto y ejemplos de código, así como un tutorial para usar la API de Twitter.

Apéndice I: Ejemplo de código API: Cómo recopilar datos de las API de búsqueda y transmisión en directo de Twitter con el paquete Rtweet

En esta sección le presentaremos brevemente un código que puede utilizar para recopilar datos históricos y en vivo de Twitter. Con solo unas pocas líneas de código, puede recopilar fácilmente datos de Twitter que sean relevantes para su contexto electoral. Después de reunir los datos objetivo, puede exportar los datos que desee a formato CSV, analizarlos en Excel o en Google Sheets, o enviárselos a un científico de datos especializado de su equipo para que busque información más a fondo. Es extremadamente útil poder recopilar datos por su cuenta en tiempo real, incluso si no tiene un científico de datos especializado en su equipo en el momento de la recopilación. Contrario a la lógica, los datos a menudo se vuelven *más* valiosos con el tiempo porque capturan desinformación, bots y actores nefarios cuyas acciones y publicaciones podrían eliminarse más tarde de la plataforma por violar los términos de servicio.

Paso 1: *Descargue R, RStudio y Rtweet*

En esta guía le enseñaremos a obtener algunos datos básicos de la API de Twitter utilizando el lenguaje de programación R. Hay un paquete específico en R, llamado *rtweet*, que facilita enormemente la obtención de datos de Twitter.

Tendrá que descargar e instalar algunos elementos para que comience a funcionar.

- Rstudio: https://www.rstudio.com/products/rstudio/download/
- R: https://www.r-project.org/

Paso 2: *Solicite una aplicación de Twitter, recupere las claves de la aplicación y cree su token*

Para recopilar datos de Twitter se utiliza una *aplicación*: este es un medio seguro de usar su cuenta para interactuar con la plataforma a través del código. En el pasado, las aplicaciones de Twitter eran gratuitas y no se necesitaba aprobación, sin embargo, hoy en día, se debe solicitar una aplicación, lo cual puede hacer aquí.

Una vez que obtenga la aplicación, deberá iniciar sesión en Twitter en un navegador y dirigirse a https://apps.twitter.com, donde puede recuperar las claves de acceso y de consumidor de su aplicación (habrá cuatro claves en total). Estas claves son simplemente cadenas de texto que su aplicación utilizará para verificar que realmente está solicitando datos en nombre de una persona, en este caso, usted. Este uso de claves para la *autenticación* es un proceso conocido como *oauth*, que significa autorización abierta. Se desarrolló como una manera de permitir que las aplicaciones realicen acciones en línea en nombre de los usuarios sin transferir su contraseña y nombre de usuario para cada acción.

Una vez que tenga sus claves y el nombre de su aplicación, puede usar el código que se muestra a continuación en la captura de pantalla para crear su "token" de autorización. Una vez creado este token, está listo(a) para comenzar a usar la API de Twitter.

```
library(rtweet)
app<-"<app name here>"
consumer_key<-"<consumer key here>"
consumer_key_secret<-"<consumer key secret here>"
access_token<-"<access token here>"
access_token_secret<-"<access token secret here>"
create_token(app,consumer_key, consumer_key_secret, access_token, access_token_secret)
```

Las líneas del código R son líneas iniciales que puede usar para autenticar su aplicación de Twitter y conectarse a la API de Twitter. Una vez que haya solicitado el acceso a una aplicación de Twitter y este haya sido aprobado, puede obtener de Twitter sus tokens de acceso y de consumidor, los cuales utilizará para autenticar su aplicación (lo que se muestra en la captura de pantalla). Una vez que su aplicación esté autenticada (es decir, Twitter sabe que la aplicación está obteniendo datos para usted y no para otra persona), ya está listo(a) para comenzar a interactuar y obtener datos de la API de Twitter.

El Dr. Mike Kearney, profesor de la Universidad de Missouri y desarrollador de rtweet, también detalla el proceso de autenticación paso a paso en el sitio web oficial de rtweet aquí.

Recopilación de datos históricos:

Con rtweet, se pueden recopilar fácilmente tuits utilizando una o varias etiquetas (*hashtags*) de interés de la API de búsqueda de Twitter. Esta API es histórica, lo que significa que recopilará datos *históricos* de los últimos 7 a 9 días correspondientes a su consulta. Las consultas son simplemente criterios que le interesa tener en los tuits que recopila y pueden contener etiquetas, palabras clave, nombres de cuenta, URL, una combinación de estos o los cuatro. En esta sección nos centraremos en las etiquetas, pero el proceso y la sintaxis son exactamente los mismos para otras entidades.

La función principal que utilizará para buscar tuits históricos se llama *search_tweets ()*.

```
my_data<-search_tweets("#ExampleHashtag", n=50000, retryonratelimit=TRUE)
```

Esta línea de código R consulta la API de búsqueda de Twitter por hasta 50,000 tuits que usen #ExampleHashtag a partir de los últimos 7 a 9 días, y guarda los resultados en una estructura de datos (dataframe) llamada "my_data". Si la etiqueta se usó menos de 50,000 veces en ese periodo, el programa arrojará un número menor de tuits. Cambiar el valor de entrada por "n" puede aumentar o disminuir la cantidad máxima de tuits que obtendrá.

```
multiple_hashtags<-search_tweets("#ExampleHashtag1 OR #ExampleHashtag2", n=50000, retryonratelimit=TRUE)
```

Esta línea de código R es similar a la consulta anterior, pero arroja hasta 50,000 tuits que contienen #ExampleHashtag1 o #ExampleHashtag2. Esta sintaxis se puede utilizar para consultar la API de búsqueda de Twitter en busca de varias etiquetas. En este código de ejemplo, los resultados se guardan en una estructura de datos llamada "multiple_hashtags". Las distintas etiquetas están separadas por lo que se conoce como "operadores booleanos", que son simplemente "Y" u "O". Use "Y" si solo quiere tuits que contengan ambas *etiquetas; "O" arrojará tuits que contengan cualquiera de las dos.*

Transmisión en directo de datos de Twitter en tiempo real:

También tiene la opción de transmitir en directo datos de Twitter en tiempo real. Esta consulta requiere que especifique en segundos el tiempo que desea transmitir en directo los tuits, así como las entidades que desea transmitir en directo (etiquetas, URL, palabras clave, @-menciones, etc.).

La sintaxis para transmitir en directo tuits en rtweet es ligeramente diferente de la que se utiliza para consultar la API de búsqueda. Al transmitir tuits en directo, se debe usar la función *stream_tweets ()*. Los distintos elementos de la consulta se separarán por comas.

```
my_streamed_data<-stream_tweets(q="#ExampleHashtag1",timeout=60)
```

```
my_streamed_data_w_multiple_hashtags<-stream_tweets(q="#ExampleHashtag1,#ExampleHashtag2",timeout=60)
```

Las figuras anteriores muestran cómo usar la función stream_tweets () de rtweet para recopilar tuits en tiempo real. La figura superior recopila los tuits usando #ExampleHashtag1 durante una ventana de transmisión en directo de 60 segundos. La figura inferior hace lo mismo, pero también recopila tuits que contienen #ExampleHashtag2.

Cómo escribir los resultados en un archivo CSV de salida:

Un formato de archivo de uso común para el análisis de datos es el archivo CSV, que son las siglas en inglés de "valores separados por comas". En un archivo CSV, cada línea representa una sola fila de la hoja de cálculo[36], y cada entidad entre comas representa una celda, o más precisamente, un valor[37] dentro de una celda.

Un archivo CSV es esencialmente una hoja de cálculo que está en un formato legible por máquina. Una vez que tenga un CSV de los tuits que ha recopilado, puede pasárselo a un científico de datos especializado para que lleve a cabo un análisis más profundo, o cargarlo en un procesador de hojas de cálculo como Microsoft Excel o Google Sheets para hacer algunos análisis por su cuenta.

36 Los científicos de datos a veces se refieren a estas filas con otros términos: *registro, instancia y observación*, que en este contexto son sinónimos de "fila" cuando se refiere a un archivo CSV.

37 Los *valores* en un csv o una hoja de cálculo a veces también se pueden denominar *campos*.

```
write_as_csv(my_data,"my_data_as_a_csv_file.csv")
```

Esta línea de código R usa el paquete rtweet para escribir una estructura de datos de tuits llamada "my_data" en un archivo CSV llamado "my_data_as_a_csv_file.csv". Después de exportar sus tuits a un archivo CSV, sus datos se pueden compartir o importar fácilmente a Microsoft Excel o Google Sheets.

Reflexiones finales

Poder extraer datos de Twitter y escribirlos en un archivo CSV es una habilidad invaluable. Incluso sin experiencia en programación, cualquier persona puede aprender el proceso que describimos aquí en menos de 2 horas, y probablemente aún más rápidamente. Una vez que tenga la capacidad de recuperar y almacenar CSV de datos relevantes de Twitter, usted y su equipo estarán en posición de analizar datos valiosos ahora y en el futuro.

Si está almacenando estos datos a largo plazo, también puede considerar comprimir el archivo en un formato .zip (u otro formato, como Tarball). Esto puede reducir la cantidad de espacio de almacenamiento necesario para almacenar el archivo y facilita la distribución del archivo a otras personas y dispositivos.

Apéndice II: Herramientas OSINT

La inteligencia de fuentes abiertas, comúnmente conocida como OSINT, es el arte de investigar una pregunta utilizando solo información y datos disponibles públicamente (o de "código fuente abierto"). En el contexto de la desinformación y el monitoreo de las redes sociales, la OSINT a menudo puede proporcionar detalles adicionales sobre actores nefarios o sospechosos en línea, incluyendo cuentas falsas o sitios web de desinformación. A continuación se muestra una lista de algunos recursos valiosos para aprender técnicas de OSINT.

- Sitio web y libro de Michael Bazzell:
  - https://inteltechniques.com
  - *Open-Source Intelligence Techniques* [Técnicas de inteligencia de fuentes abiertas]
- Kit de herramientas de investigación en línea de Bellingcat: https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICK0GguA/edit
- Lista pública de herramientas de verificación y OSINT del periodista de BuzzFeed, Craig Silverman: https://docs.google.com/document/d/1ZJbIUk5L8fe3VKK9CLVNMj9qOFdXG-RhQT6pyEgsS4I/edit
- Comprop Navigator, publicado por el proyecto de Propaganda Computacional del Instituto de Internet de Oxford, compila métodos y herramientas OSINT relacionadas con la desinformación y otras investigaciones en línea. https://navigator.oii.ox.ac.uk/
- Primer borrador de la guía sobre recopilación y monitoreo de noticias en las redes sociales https://firstdraftnews.org/wp-content/uploads/2019/10/Newsgathering_and_Monitoring_Digital_AW3.pdf?x36710
- Fighting Disinformation Online: A Database of Web Tools, hosted by the Rand Corporation. https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html
- *Verification Handbook for Disinformation and Media Manipulation* [Manual de verificación de desinformación y manipulación de medios] https://datajournalism.com/read/handbook/verification-3/

Referencias

Allcott, H., Gentzkow, M., & Yu, C. (2018). *Trends in the Diffusion of Misinformation on Social Media*. https://web.stanford.edu/~gentzkow/research/fake-news-trends.pdf

Borgatti, S., Everett, G., & Johnson, J. (2013). *Analyzing Social Networks*.

Democracy Reporting International. (Octubre de 2019) *Guide for Civil Society on Monitoring Social Media During Elections*. https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf

Jack, C. (2017). *Lexicon of Lies.* Data & Society. https://datasociety.net/output/lexicon-of-lies/

Monaco, N. (2019). *Welcome to the Party: A Data Analysis of Chinese Information Operations.* Obtenido de https://medium.com/digintel/welcome-to-the-party-a-data-analysis-of-chinese-information-operations-6d48ee186939

Instituto Nacional Demócrata para Asuntos Internacionales (Mayo de 2019) *Disinformation and Electoral Integrity: A Guidance Document for NDI Elections Programs*. https://www.ndi.org/publications/disinformation-and-electoral-integrity-guidance-document-ndi-elections-programs

Instituto Nacional Demócrata para Asuntos Internacionales (Diciembre de 2018). *Apoyando la integridad de la información y el discurso político civil*. https://www.ndi.org/sites/default/files/Spanish%20Supporting%20Information%20Integrity.pdf

Pakzad, R., & Salehi, Ni. (2019). *Anti-Muslim Americans: Computational Propaganda in the United States. Institute from the Future*. Obtenido de http://www.iftf.org/fileadmin/user_upload/downloads/ourwork/IFTF_Anti-Muslim_comp.prop_W_05.07.19.pdf

Russell, M., & Klassen, Mikhail. (2018). *Mining the social web.* Sebastopol, CA: O'Reilly Media.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Consejo Europeo. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Woolley, S., Pakzad, R., & Monaco, N. (2019). *Incubating Hate: Islamophobia and Gab.* German Marshall Fund. http://www.gmfus.org/sites/default/files/publications/pdf/Incubating%20Hate%20-%20Islamophobia%20and%20Gab.pdf

Woolley, S., & Howard, P. (2017). *Computational Propaganda Worldwide: Executive Summary.* Artículo de trabajo. 2017.11. Oxford, R.U.: Proyecto sobre propaganda computacional. http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

Zeiter, K., Pepera, S., Middlehurst, M., Ruths, D. (2019). *Tweets That Chill: Analyzing Online Violence Against Women in Politics*. Instituto Nacional Demócrata para Asuntos Internacionales. https://www.ndi.org/tweets-that-chill

NATIONAL
DEMOCRATIC
INSTITUTE

NDI.ORG