DATNAV

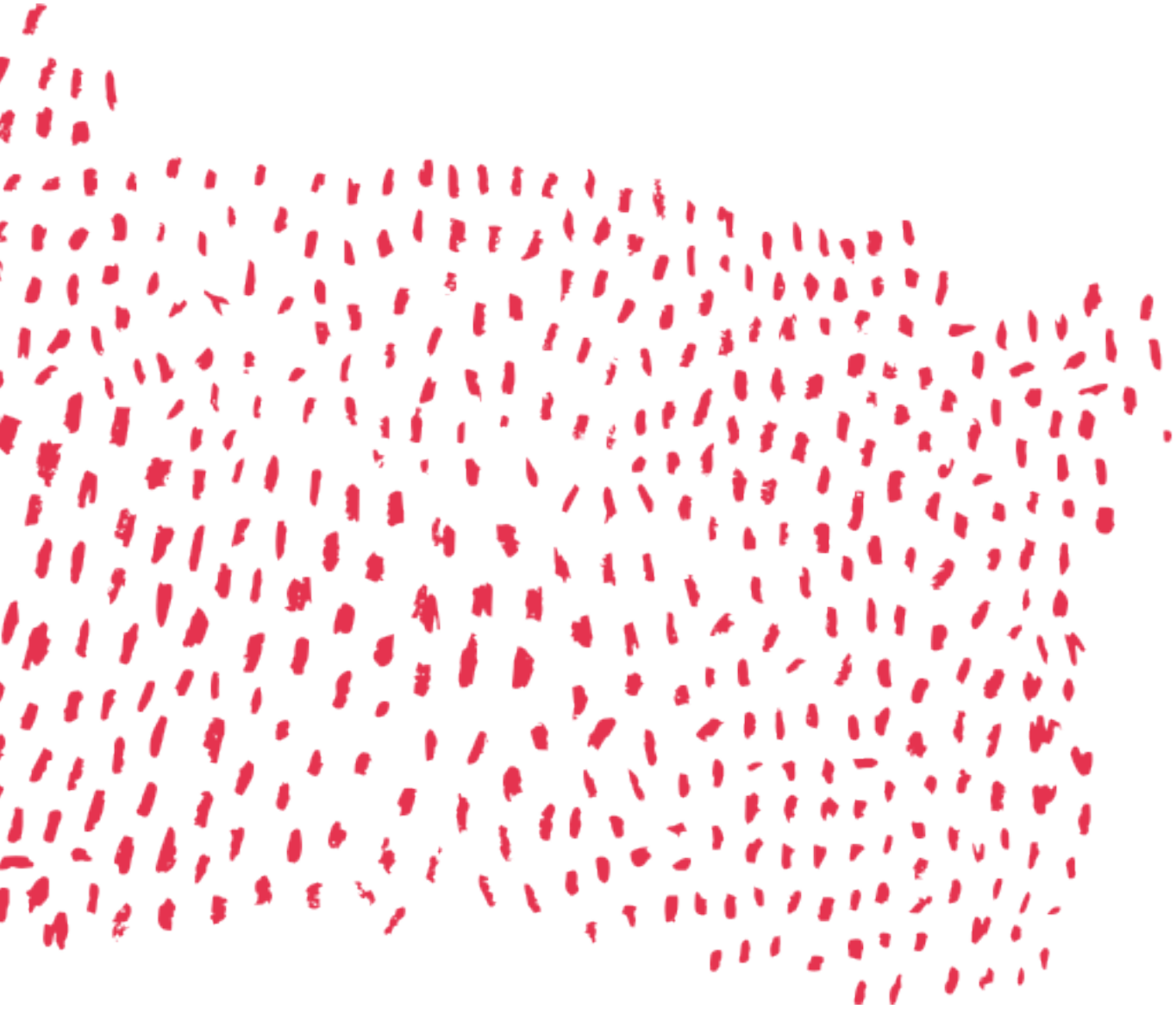
Cómo navegar entre datos digitales para la investigación de derechos humanos

THE ENGINE ROOM

benetech
TECHNOLOGY SERVING HUMANITY

AMNESTY INTERNATIONAL

Hivos
people unlimited



Center for Economic and Social Rights

CGHR Centre of Governance and Human Rights

Eyewitness Media Hub

E·S·R·C Economic & Social Research Council

University of Essex

Gulf Center for Human Rights

The Human Rights, Big Data and Technology Project

HRDAG Human Rights Data Analysis Group Everybody Counts.

Syria Justice and Accountability Centre

WITNESS See It Film It Change It

Colaboradores

Les queremos dar las gracias a los siguientes **colaboradores durante el sprint de escritura**:

- Allison Corkery, Center for Economic and Social Rights
- Sam Dubberley, Eyewitness Media Hub y Human Rights, Big Data and Technology Project, Universidad de Essex
- Scott Edwards, Amnesty International
- Lisa Gutermuth
- Danna Ingleton, Amnesty International
- Christoph Koettl, Amnesty International
- Jule Krüger, Human Rights Data Analysis Group (HRDAG)
- Chris Michael, Collaborations for Change
- Ella McPherson, Departamento de Sociología y el Centro de Gobernanza y Derechos Humanos, Universidad de Cambridge
- Shabnam Mojtahedi, Centro de Justicia y Responsabilidad de Siria
- Chitra Nagarajan
- Zara Rahman, The Engine Room
- Elsa Saade, Gulf Center for Human Rights
- Collin Sullivan, Benetech
- Jackie Zammuto, WITNESS

También damos las gracias a las siguientes **personas que contribuyeron al proyecto como revisores** de este documento, participantes llamamiento abierto a la comunidad, y entrevistados durante la fase temprana de este proyecto:

- Kristin Antin, HURIDOCS
- Jay Aronson, Centro por los Derechos Humanos, Carnegie Mellon
- Patrick Ball, HRDAG
- Alexis Bautista, Migrant Forum in Asia
- Anh Bui, Benetech
- Neil Blazevic, East and Horn of Africa Human Rights Defenders Project
- Laura Carter, Amnesty International
- Kristy Crabtree, International Rescue Committee
- Elsa Marie da Silva, SafeCity
- Priti Darooka, Programme on Women's Economic, Social and Cultural Rights
- Jessica Dheere, SMEX
- Nicola Diday, swisspeace
- Tarek Dobo, Centro de Justicia y Responsabilidad de Siria
- John Emerson, NYU Center for Human Rights and Global Justice
- Wael Eskandar
- Emmanuel Freudenthal
- Mahbul Haque , Bangladesh Centre for Human Rights and Development
- Morgan Hargrave, WITNESS
- Theresa Harris, AAAS
- Shevy Korzen, The Public Knowledge Workshop
- Tom Longley
- Milena Marin, Amnesty International
- Beatrice Martini, Aspiration
- Ruth Miller
- Tawanda Mugari, Digital Society of Zimbabwe
- Yvonne Ng, WITNESS
- Dan O'Clunaigh
- Ted Perlmutter, Institute for the Study of Human Rights at Columbia University
- Robin Pierro, European Inter-University Centre for Human Rights and Democratization
- Enrique Piraces, RightsLab

- Vanya Rakesh, CIS India
- Vijay Rao,
  Centro de Justicia y Responsabilidad de Siria
- Anja Reiss
- Mike Romig
- Bridget Rutherford, PILPG
- Stephanie Seale, Benetech
- Marizen Santos, Migrant Forum in Asia
- Ryan Schlief, International Accountability Project
- Samaruddin Stewart
- Tom Trewinnard, Meedan
- Bert Verstappen, HURIDOCS
- Friedhelm Weinberg, HURIDOCS
- Eeva Moore
- Solana Larsen

Esta obra está licenciada bajo la licencia Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0). Para ver una copia de esta licencia, visite:
http://creativecommons.org/licenses/by-sa/4.0/

Ilustración para la portada: Lynne Stuart.
Diseño gráfico: Federico Pinci.

Primera edición: junio de 2016.

ÍNDICE

Empezando

Introducción 8
Esta guía es para ti 9
Nuevas posibilidades con los datos digitales 10
¿Cuándo se deben usar los datos digitales? 14
Cómo obtener apoyo dentro de tu organización 19

Comprender la verificación y documentación

¿Qué son los metadatos? 22
Verifica, verifica, verifica 24
Datos de redes sociales 32
Datos que se sostendrán en un tribunal 36

Técnicas prácticas

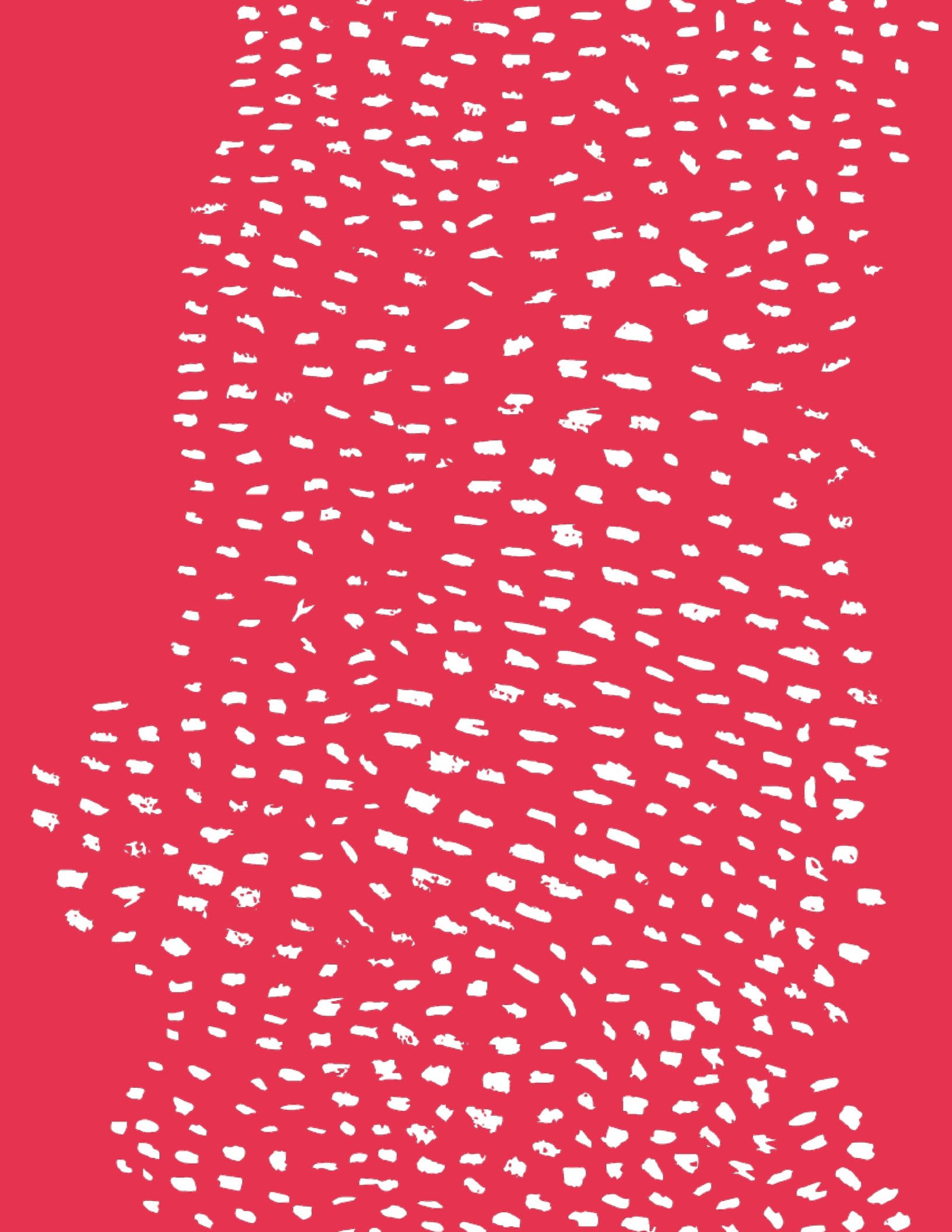
Estadísticas de Gobierno Abierto 40
Datos de presupuestos para derechos humanos 44
Hoy está, mañana quizás no: Preservando vídeos y fotos en línea 48
Organizando su catálogo de fotos y vídeos 51
Como se ve desde el cielo: Satélites y drones 55

Consideraciones de datos responsables

Riesgos de seguridad de la vida real 61
Datos Responsables 63
¿Son seguras tus herramientas digitales? 65
Trauma secundario y TEPT 69

A dónde ir desde aquí

Cómo encuadrar tu investigación 74
Conclusión 79
Recursos y lectura adicional 81



Empezando

Empezando

INTRODUCCIÓN

Desde vídeos en línea que muestran violaciones de derechos, a imágenes satelitales de daño ambiental o a relatos de testigos presenciales diseminados en medios sociales, hoy tenemos acceso a datos relevantes más que nunca. Cuando se usan de manera responsable, estos datos pueden ayudar a los profesionales defensores de los derechos humanos ante un tribunal, en el trabajo con representantes del gobierno y periodistas o bien para documentar e incorporar al registro histórico.

Obtener, difundir y almacenar datos digitales también se está volviendo cada vez más económico. En la medida de que los costos continúan reduciéndose y se desarrollan nuevas plataformas, crecen las oportunidades de explotar estas fuentes de datos para el trabajo en defensa de los derechos humanos.

Pero integrar la captura y administración de datos digitales en el día a día del trabajo de investigación y documentación en derechos humanos puede ser desafiante, incluso apabullante, para individuos y organizaciones. Esta guía está diseñada para ayudarte a manejar e integrar nuevas formas de datos en tu trabajo en derechos humanos.

Esta guía es el resultado de una colaboración entre Amnistía Internacional, Benetech y The Engine Room, que comenzó a finales de 2015. Hemos llevado a cabo una serie de entrevistas, consultas a la comunidad y sondeos, para comprender si los datos digitales estaban siendo integrados en el trabajo en derechos humanos. En la gran mayoría de casos hemos encontrado que no existía integración y nos preguntamos ¿por qué?

Principalmente, los investigadores en derechos humanos parecían estar abrumados por la multitud de posibilidades. Frente a recursos limitados, al no saber cómo empezar o si valdría la pena, la mayoría de los entrevistados se abstuvieron de siquiera intentar reforzar su tarea diaria utilizando recursos digitales.

Para dar apoyo a todos los que trabajan en el campo de los derechos humanos para explorar este entorno complejo, hemos reunido a un grupo de 16 investigadores y expertos técnicos en un castillo en las afueras de Berlín, Alemania, en mayo de 2016 para redactar esta guía a lo largo de cuatro días de intensa reflexión y escritura.

ESTA GUÍA ES PARA TI

Vamos a asumir que ya sabes cómo realizar investigación en derechos humanos, pero deseas expandir tu conocimiento sobre cómo usar datos digitales y medios en línea para propósitos de documentación.

Esta es una introducción amplia que te pondrá en buen camino para formular tus propias preguntas y buscar tus propias soluciones. Apuntamos a promover un pensamiento crítico en lugar de ser prescriptivos en cuanto a qué software, dispositivos, o plataformas específicas deberías usar, ya que estas evolucionan constantemente.

Hemos examinado recursos y recopilado lectura adicional sobre las áreas abordadas en este informe, que puedes encontrar disponibles en ***https://engn.it/datnav***.

Imaginamos que eres un investigador en derechos humanos, periodista, estudiante, diseñador de políticas o filántropo, y que buscas...

- Mejorar la investigación y documentación tradicionales (entrevistas, encuestas, y hojas de cálculo) aprendiendo a incorporar datos digitales.
- Construir conocimiento y pericia anticipando a una futura emergencia, de manera de evitar recopilar información de forma convencional cuando se produce un evento o violación de derechos.
- Comprender las oportunidades, límites y riesgos de los recursos digitales, además de cuándo y cómo buscar consejo experto para ayudarte a alcanzar tus metas.
- Superar el temor a los datos digitales y su tecnología, que ya tus colegas y tus adversarios ya los utilizan de forma intensiva. Con mejores herramientas, sabes que puedes ser más eficiente.

NUEVAS POSIBILIDADES CON LOS DATOS DIGITALES

Algunas **formas de datos digitales** discutidas en esta guía:

- Fotos, vídeos, y sus metadatos
- Imágenes satelitales e información geoespacial
- Motores de búsqueda, redes sociales, y opiniones en línea
- Estadísticas y presupuestos gubernamentales

Hoy, millones de personas tienen la capacidad de tomar fotografías y vídeo de alta resolución con dispositivos que caben en sus bolsillos. Pueden compartir con facilidad lo que han capturado con audiencias cercanas y lejanas, proyectando lo que han visto de a través del espacio y el tiempo, generalmente sin importar las fronteras o el idioma.

Para los investigadores en derechos humanos, estas nuevas formas de compartir información están cambiando el modo en que descubrimos la información relevante, y hacen necesaria la verificación y el uso de un saludable escepticismo.

Comparado con hace sólo unos pocos años, hoy tenemos inmensas posibilidades que nacen de la abundancia de datos y fuentes, que son útiles al trabajo en defensa de los derechos humanos. Los datos digitales pueden sustentar un registro documental profundo, amplio, preciso y eficiente de situaciones relativas a los derechos humanos.

Primero, pueden resultar una nueva fuente de evidencia que corrobora la documentación tradicional de eventos específicos. Las violaciones de los derechos humanos a menudo se tipifican por un evento. Contando con nuevas fuentes de datos, la cantidad de detalles que pueden ser descubiertos acerca de un determinado evento crece (es decir, el quién, qué, dónde y cuándo, pueden identificarse de forma más específica), igual que lo hace el impacto del hallazgo de los hechos.

Segundo —y quizá de modo incluso más significativo— los datos proporcionan una unidad de medida estandarizada que puede ser capturada, categorizada y comparada entre grupos y a lo largo del tiempo. Esto los hace útiles para descubrir tendencias y patrones que ayudan a sacar a relucir disfunciones de carácter más sistémico.

Redefinición de métodos tradicionales

La documentación de situaciones de derechos humanos tradicionalmente ha implicado entrevistar a víctimas y testigos, y reunir evidencia que sustente los hechos. Se centra en un evento o incidente específico. El objetivo es averiguar qué ocurrió, a quién, por quién, dónde, cuándo, y cómo.

Responder a estas seis preguntas es bastante directo cuando los gobiernos violan una obligación negativa (la obligación a no hacer algo). Son ejemplos la tortura, los arrestos arbitrarios, la represión de protestas pacíficas, los desalojos forzados, o las esterilizaciones sin consentimiento. Sin embargo, las preguntas (qué, a quién, por quién, dónde, cuándo, y cómo) a menudo son más difíciles de responder en el caso de las obligaciones positivas.

Las obligaciones positivas requieren que el gobierno actúe. Puede consistir en que el gobierno salga de la inacción, o que haga *algo de forma diferente*. Un gran número de violaciones de los derechos humanos —en particular de los derechos económicos, sociales, y culturales— entran en esta segunda categoría. Son ejemplos el tráfico de seres humanos, la explotación laboral, la brutalidad policial, la desnutrición, la indigencia, el analfabetismo, y las enfermedades prevenibles.

Estos tipos de violaciones de derechos son complejas y están profundamente enraizadas. No se limitan a un evento o incidente específico. Al contrario, resultan de disfunciones sistémicas en las formas en las que se diseñan e implementan leyes, políticas y regulaciones, que los métodos de documentación tradicionales tienen dificultad para hacer evidentes. Estas disfunciones pueden ser causadas por un gran número de actores y factores, lo que que hace que sea difícil determinar quién es el responsable.

Una aproximación más amplia al proceso de documentación puede ayudarle a arrojar luz sobre los actores y factores que influyen en el modo en que leyes, políticas y regulaciones impactan en grupos de forma concreta.

Caso de estudio

Mejorando el uso de datos para documentar violaciones en Siria

En abril de 2011, un grupo de activistas en Siria comenzaron a observar y documentar sistemáticamente las violaciones de derechos humanos, recopilando y revisando vídeos en línea sobre violencia y atrocidades. Cuando varias personas del equipo fueron secuestradas, los miembros restantes se lanzaron a mejorar la seguridad, los métodos y las colecciones de datos tras la consulta con expertos.

En un momento dado, fundaron una organización sin fines de lucro llamada ***The Violations Documentation Center (VDC)*** donde ahora recopilan datos sobre encarcelamientos, torturas, desapariciones y asesinatos de civiles y rebeldes y de las fuerzas del régimen en Siria, usando rigurosos métodos de verificación, de modo que su documentación potencialmente pueda ser utilizada en eventos de justicia transicional cuando finalice el conflicto.

Tienen más categorías más detalladas en su base de datos, más opciones de filtrado durante la búsqueda, y hacen un mejor uso de imágenes satelitales para corroboración. “Ahora nuestra información se usa como fuente confiable por representantes de la ONU, gobiernos y defensores de los derechos humanos de todo el mundo, ya que tenemos la certeza de que nuestros datos son completos”, dice un representante de VDC.

Foto: ***Damascus***, por ***Игорь*** M, con licencia CC-BY-SA 2.0..

Caso de estudio

Investigación de matanzas masivas en Burundi

Los cuerpos de al menos 70 personas ejecutadas por las fuerzas del gobierno en Burundi, en diciembre de 2015, desaparecieron misteriosamente provocando rumores de un enterramiento masivo.

Un investigador de campo de Amnistía Internacional pasó 10 días tomando fotos y entrevistando a testigos tras las matanzas, pero eran necesarias más evidencias.

Las fotos satelitales probablemente podrían ayudar a localizar una fosa, si al menos supieran dónde mirar. Por fortuna, Amnistía Internacional recibió un vídeo de un contacto en Burundi que mostraba el presunto sitio del enterramiento. Se consultaron en línea las coordenadas exactas en Google Earth, y al fin las imágenes satelitales mostraron verazmente tierra removida en el punto identificado.

El hallazgo de un enterramiento masivo vía satelital atrajo una gran cobertura mediática y ayudó a crear presión política. Diez años atrás Amnistía Internacional no habría tenido tal vídeo, ya que la gente en Burundi no habría tenido teléfonos móviles con cámara. Gracias a la evolución de la tecnología, los investigadores ahora tienen muchas más herramientas que incorporar a su trabajo de campo tradicional.

Foto: Imagen de satélite mostrando tierra removida en la zona de Buringa, lo que es consistente con declaraciones de testigos y grabaciones de vídeo que recogen enterramientos masivos. ©DigitalGlobe 2016.

Para que cualquier dato sea útil en la documentación de situaciones de derechos humanos, debe poder verse el lugar de donde vino, cuándo fue creado, quién lo creó, y por qué. Lugar, Momento, Persona, Motivación

Empezando

¿CUÁNDO SE DEBEN USAR LOS DATOS DIGITALES?

Si estás más acostumbrado a la investigación y documentación con medios y métodos tradicionales, puede ser desalentador dedicar tiempo a evaluar si los datos digitales o el contenido de las redes sociales es merecedor de tu atención.

Esta sección enumera siete preguntas para ayudarte a ponderar el valor neto de nuevos tipos de datos en el contexto particular de tu investigación. ¿Serán de verdadera ayuda?

Necesitamos sopesar constantemente los pros y contras, incluyendo el costo, ahorro, y ***riesgos de hacer un mal manejo de los datos***. Por ejemplo, el riesgo a ser vigilado puede hacer que la recopilación de datos digitales sea inconveniente en algunos casos, o puede que sólo tengas acceso a algunas poblaciones y no a otras, distorsionando el resultado de tu investigación.

En realidad, no es tan distinto de los métodos de investigación tradicionales. La parte más ardua es pensar de forma creativa acerca de qué datos pueden existir (especialmente los que fueron creados para otros propósitos) y valorar si tu y tu equipo pueden recopilarlos y manejarlos de forma efectiva.

Siete puntos a considerar antes de usar datos digitales para trabajos en derechos humanos

1. ¿Ayudarían los datos digitales a responder de manera genuina a tus preguntas de investigación? ¿Cuáles son los pros y contras de la fuente o medio en particular? ¿Qué podrías aprender de pasados usos de tecnología similar?
2. ¿Qué fuentes es probable que estén recogiendo o capturando el tipo de información que buscas? ¿Cuál es el contexto en que esta información se viene produciendo y utilizando? ¿Serán receptivas a este tipo de datos las personas u organizaciones hacia las que se orienta tu trabajo?
3. ¿Con qué facilidad se integrarán las nuevas formas de datos en la dinámica de trabajo de tu organización? ¿Tienes realmente el tiempo y el dinero para recopilar, almacenar, analizar, y especialmente, para verificar estos datos? ¿Puede alguien de tu equipo dar soporte a esa tecnología con facilidad?
4. ¿Quién posee o controla los datos que vas a usar? ¿Compañías, gobiernos, adversarios? ¿Hasta qué punto es difícil obtenerlos? ¿Es un método de recopilación legítimo o legal? ¿Cuál es la posición interna sobre esto? ¿Tienes consentimiento informado real de los individuos?
5. ¿Cómo afectarán a la representatividad de distintas poblaciones las barreras digitales y las diferencias en el acceso local a plataformas en línea, computadoras o teléfonos? ¿Podrían las conclusiones basadas en esos datos terminar reforzando las desigualdades, estereotipos o puntos ciegos?
6. ¿Son suficientemente robustos los protocolos de confidencialidad y seguridad en la comunicación digital y manejo de datos en tu organización? ¿Pueden mitigar los riesgos para ti, tus asociados, y sus fuentes? ¿Se actualizan con suficiente frecuencia las herramientas y procesos de seguridad?
7. ¿Tienes medidas de contingencia en orden para afrontar o evitar los traumas secundarios que tu o tus asociados puedan experimentar al ver contenidos digitales perturbantes, tanto a nivel personal como a nivel de toda la organización?

Ejemplos prácticos

Aquí tiene algunos ejemplos hipotéticos para mostrar distintas fuentes y usos de los datos digitales.

Escenario

Refugiados a quienes se deniega el acceso a atención sanitaria | ¿Debemos usar datos digitales?

Deseas investigar alegaciones sobre denegación de acceso a atención sanitaria a refugiados en tránsito, y estás considerando usar fotografías satelitales para cartografiar rutas de viaje recientes, y contenido de redes sociales para buscar testimonios y entrevistar sujetos.
Tienes un presupuesto muy limitado y no has usado antes esta clase de datos, pero sabes que la mayoría de los refugiados tienen teléfonos móviles y usan redes sociales para compartir información. Tu mayor preocupación es que los datos de geolocalización puedan acabar en manos de grupos de vigilantes y que éstos que ataquen a los inmigrantes. De hecho, a causa de estos grupos, los refugiados han trasladado cada vez más sus comunicaciones desde plataformas públicas como Twitter a grupos de conversación más cerrados en Facebook y WhatsApp.

¿Qué hacer?

Decides obtener acceso a esos grupos cerrados de redes sociales mediante tus contactos, y asegurarte que la seguridad de todos aquellos con los que te comuniques en línea sea la máxima prioridad.
Consultas a individuos y grupos acerca de las denegaciones de acceso a atención sanitaria.
Por ahora, descartas el uso de fotos aéreas.

PREGUNTA DE INVESTIGACIÓN:
¿Se está denegando el acceso a atención sanitaria a inmigrantes en el País X?

El País X es punto de entrada a la Unión Europea para refugiados. Existen informes de violaciones al derecho de acceso a atención sanitaria para determinados refugiados que entran por mar. Este caso de estudio asume que el investigador no conoce exactamente por dónde entran los refugiados.

VIOLACIONES DE DERECHOS SANITARIOS CON LOS REFUGIADOS

TIPOS DE DATOS POTENCIALES

- DATOS DE SATÉLITE
- BASES DE DATOS GEOESPACIALES
- INFORMACIÓN METEOROLÓGICA
- DATOS ABIERTOS[a]
- INFORMACIÓN DE LA GENTE[b]
- MUESTRAS DE DATOS ALEATORIAS TOMADAS DE CENTROS MÉDICOS[c]
- DATOS DE REDES SOCIALES 'CERRADOS'[d]
- INFORMATIÓN AÉREA NO-SATELITAL
- INFORMACIÓN PRESUPUESTARIA DEL GOBIERNO[e]
- INFORMACIÓN A TRAVES DE REDES SOCIALES
- DATOS DE CORRIENTES OCEÁNICA[f]

a De organizaciones humanitarias y otros socios potenciales (como información de atención sanitaria, análisis de nacimientos, etc.).

b Tales como mapas de reportes de ciudadanos relacionados con incidentes que involucran refugiados en el punto de entrada.

c Estructuras que proporcionan apoyo médico a refugiados.

d Tales como grupos de Facebook y Whatsapp usados por refugiados para comunicación de apoyo en ruta o asuntos de seguridad.

e Asignaciones para el apoyo médico a refugiados.

f O bien otros factores que pueden afectar el movimiento de refugiados

Escenario

Rastrear censura en Internet | ¿Debemos usar datos digitales?

Te encuentras trabajando en un país donde se sabe que el gobierno clausura el acceso a Internet durante protestas y turbulencias sociales, y deseas documentar esto. Descubres que puedes acceder en línea a los registros de *interrupción de servicio de Google* que te permitirían identificar probables episodios de cortes de servicio que puedes luego referenciar de forma cruzada con otras fuentes de información. Sin embargo, el gobierno tiene capacidad de vigilancia digital y de Internet, y podría rastrear la actividad de tu navegador y el historial de búsqueda hasta dar contigo, identificándote como un activista en defensa de los derechos humanos.

¿Qué hacer?

Dado el historial de vigilancia del gobierno, tu organización te ha instruido en el uso de *VPNs (redes privadas virtuales)* cuando haces búsquedas y te comunicas en línea. Decides que puede ocultar suficientemente tus rastros digitales y realizar la investigación a pesar de los riesgos.

PREGUNTA DE INVESTIGACIÓN:
¿Violó el gobierno del País Y los derechos de libertad de expresión y de acceso a la información al impedir acceder a Internet?

Ha habido una ola de protestas públicas en el País Y durante el pasado año. Recientemente esto llegó a un punto crítico en una protesta masiva que bloqueó el centro de la capital. Los activistas informaron de que el gobierno bloqueó el acceso a Internet para sofocar las protestas y evitar que la información llegase a otros actores fuera del país.

VIOLACIONES DE DERECHOS EN INTERNET

TIPOS DE DATOS POTENCIALES

- REGISTROS DE LA COMPAÑÍA DE SERVICIOS DE INTERNET
- INFORMES DE LOS MEDIOS DE COMUNICACIÖN
- REGISTROS DE DESCARGA DE NUEVAS APLICACIONES[a]
- ANÁLISIS DE VELOCIDAD DE INTERNET
- DECLARACIONES DEL SECTOR PRIVADO/ONGs[b]
- PETICIONES DE REMOCIÖN DE CONTENIDOS O DE BLOQUE DE USUARIOS[c]
- ESTADÍSTICAS DE TRÁFICO EN INTERNET[d]
- REDES SOCIALES
- REGISTROS TELEFÓNICOS[e]
- BLOQUEO DEL ACCESO A INTERNET POR PARTE DEL GOBIERNO[f]
- DATOS DE PSIPHON

a En particular los que se consideran seguros y accesibles.

b Declaraciones de compañías privadas (como WhatsApp) y organizaciones de derechos humanos.

c Reportados por compañías de redes sociales.

d De tráfico general o de sitios web específicos.

e Datos de uso de teléfonos móviles.

f Para sofocar protestas.

Escenario

Violación del derecho de acceso al agua | ¿Debemos usar datos digitales?

Las fotos aéreas junto a ríos en una región específica muestran lo que parecen ser barreras físicas para acceder al agua. Como principal fuente de agua para los lugareños, te preocupa que la compañía esté violando los derechos de acceso al agua de la población local. La población que vive en las riberas de los ríos tiende a ser más pobre, aunque la mayoría tiene teléfono móvil. Te gustaría distribuir un sondeo mediante SMS preguntando si su acceso al agua está siendo limitado y dónde, pero la población ha participado ya de muchos programas de desarrollo en los últimos años y sabes que están un tanto cansados de sondeos. Tu ONG es joven y tiene recursos limitados.

¿Qué hacer?

Aunque el sondeo SMS te permitirá llegar a tu población objetivo, el contexto puede evitar que obtengas respuestas. Dado que (1) tu objetivo es una población pobre cansada de sondeos, que (2) tendrás que pedir a cada persona que responda que pague por el mensaje de respuesta, y que (3) tu ONG tiene un nombre con poco reconocimiento, te das cuenta de que esto podría ser dura batalla. Decides pedir a un colega en una ONG bien establecida que te presente a un líder comunitario para que puedas explicarle el proyecto, pedir la contribución de la comunidad en el diseño de la encuesta, y encontrar la forma de devolver a la comunidad la información que resulte del proyecto que llevas a cabo.

PREGUNTA DE INVESTIGACIÓN:
¿Es responsable FPower de la contaminación delsuministro de agua?

En el País X hay altos niveles de desnutrición infantil en entornos de ingresos bajos, debido a la disentería. También hay muchas operaciones de agricultura intensiva localizadas cerca de los ríos por todo el país. La mayoría de las explotaciones son propiedad de un grupo de compañías: FPower. El consejo de dirección de FPower tiene dos miembros directamente relacionados con ministros del gobierno.

VIOLACIONES DEL DERECHO DE ACCESO AL AGUA

TIPOS DE DATOS POTENCIALES

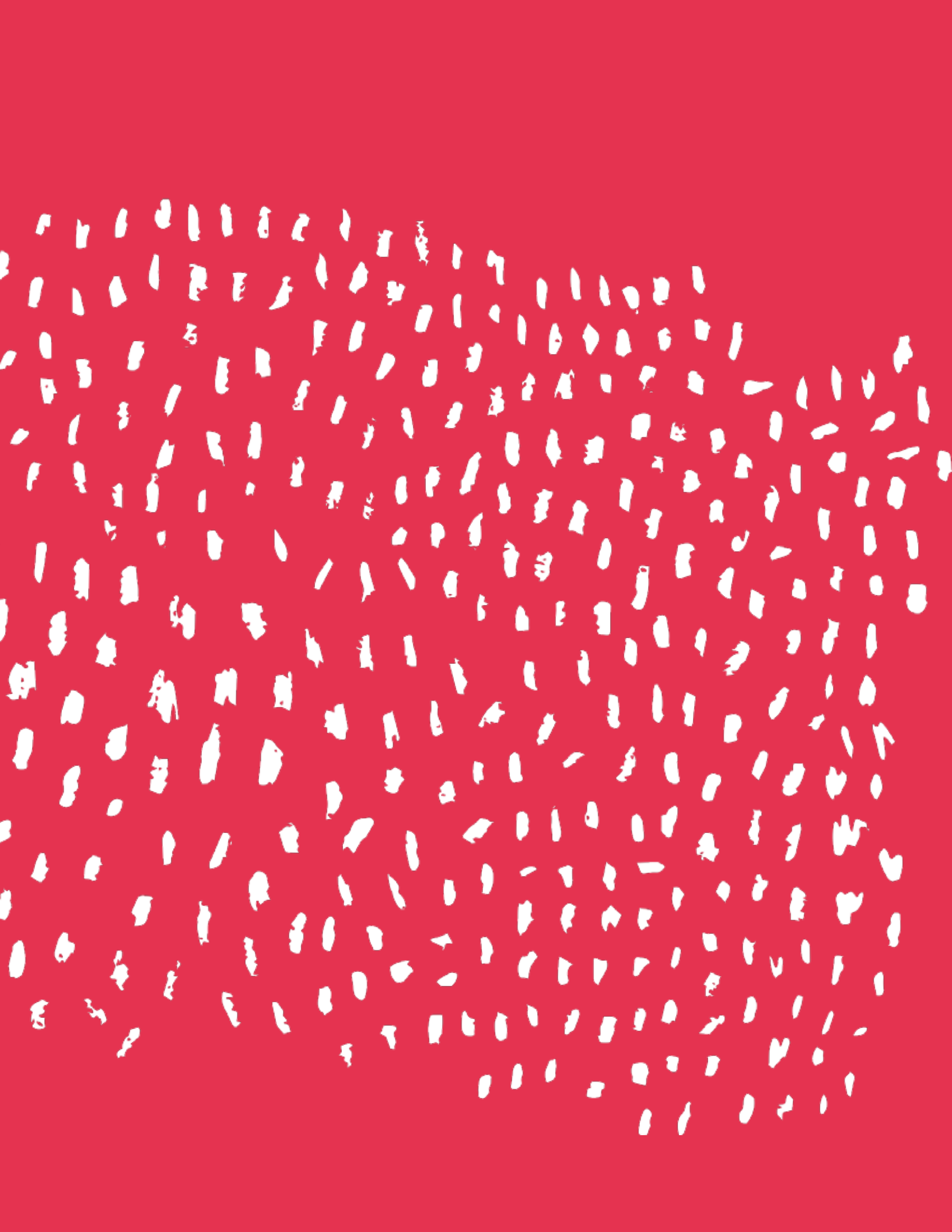
- ESTADÍSTICAS NACIONALES DE SALUD
- BÚSQUEDAS EN INTERNET / ANÁLISIS DE DATOS
- INFORMACIÓN DE OPERACIONES Y LOCALIZACIÓN DE EMPRESAS
- SONDEO VIA SMS DE CONSUMO DE CALORÍAS
- SUPERPOSICIÓN DE DATOS GEOGRÁFICOS Y TEMPORALES
- FOTOGRAFÍAS O IMÁGENES SATELITALES[a]
- DATOS DE PRESUPUESTOS[b]
- DATOS SOBRE PROVISIÓN DE SERVICIOS[c]
- ANÁLISIS DE CONTAMINACIÓN DEL AGUAS

a De intervalos de tiempo (time-lapse) o geoespaciales.
b Gasto del gobierno en programas de nutrición.
c Del gobierno o de agencias humanitarias.

CÓMO OBTENER APOYO DENTRO DE TU ORGANIZACIÓN

Incluso donde hay apetito por el cambio, las largas jornadas de trabajo y los presupuestos ajustados pueden provocar que individuos y organizaciones queden sujetos al viejo modelo de hacer las cosas. Por tanto, para incorporar las modernas prácticas de datos el liderazgo de la organización tiene que abanderar el cambio. Aquí tienes **diez puntos a incluir en un debate con los directores**, para ayudarles a ver la necesidad del cambio.

1. **Realidad del mercado:** Muchas organizaciones de defensa de los derechos humanos ya se encuentran trabajando con datos digitales, aunque muchas lo hacen sin invertir en alfabetización digital. No desarrollar las destrezas internas necesarias dentro de tu organización pone en riesgo la relevancia de tu trabajo.
2. **Presupuesto:** Muchas de las herramientas recomendadas son de bajo coste o gratuitas.
3. **Instrucción:** Sí, la formación lleva tiempo, pero los empleados valoran el aprendizaje. Existe investigación que muestra que la importancia que los empleados dan a las nuevas oportunidades de capacitación en el trabajo se encuentra en segundo lugar, tras la retribución. Especialmente para pequeñas organizaciones, mantener el personal y reducir la tasa de reemplazo es vital. Entidades como School of Data o Advocacy Assembly ofrecen cursos en línea gratuitos.
4. **Atractiva para nueva contratación:** Ser una organización que mira hacia delante y utiliza nuevas herramientas ayuda a atraer a los mejores profesionales del sector.
5. **Impacto:** Usar los nuevos datos de forma eficiente puede mejorar los resultados y permitir una mejor observación de la realidad respecto de violaciones de derechos humanos.
6. **Financiación:** A Los donantes les interesa la utilización de datos digitales y su aplicación en reportes de derechos humanos, y realizan llamamientos para propuestas de financiación en base a ello.
7. **Impulso de la marca:** Ubican a la marca como una organización capaz, visionaria, y deseosa de implicarse en nuevos proyectos.
8. **Misión:** La misión es observar, informar y elevar la percepción sobre violaciones de derechos humanos. Usados de forma apropiada, los datos digitales permiten a las organizaciones hacer esto aún mejor.
9. **Charlas cortas para el personal:** Invita a alguien que trabaje con éxito con datos digitales a dar una charla corta acerca de lo que están haciendo.
10. **Construir redes entre pares:** Construir relaciones orientadas a los datos con organizaciones semejantes para compartir las mejores prácticas.



Comprender la verificación y documentación

¿QUÉ SON LOS METADATOS?

Los metadatos son información acerca de un archivo (tal como un documento word, un PDF, una imagen, un archivo de música, etc.) que se almacenan dentro del propio archivo, ocultos a la vista.

Esta información puede incluir la fecha y hora en que fue creado el archivo, el nombre de usuario utilizado por quien lo creó o editó, información acerca del dispositivo que lo creó, y otros tipos de información. En otras palabras, los metadatos de un archivo podrían revelar quién creó ese archivo. Esta información es generada automáticamente por dispositivos como cámaras, computadoras, y teléfonos, pero también puede ser editada y manipulada por quienes saben cómo hacerlo. Esto puede ser algo

bueno, si quiere que la información sea privada al compartir archivos, pero los riesgos son obvios si está tratando con verificación de información sensible de derechos humanos.

Tomemos las fotos como ejemplo. Cuando tomas una foto con tu cámara digital, ¿qué ocurre? Si tu cámara o teléfono sabe dónde estás, esa información (en forma de coordenadas GPS) se puede guardar en los metadatos del archivo. Si tu cámara sabe qué hora es, registra la fecha y hora en que fue tomada la foto. Si tu cámara o teléfono tiene un número de serie, también puede ser registrado en los metadatos.

Los archivos de imagen digital como TIFF (Tagged Image File Format) y JPEG (Joint Photographic Experts Group) creados por cámaras digitales o smartphones, contienen metadatos en un formato llamado EXIF (Exchangeable Image File Format) que podría incluir toda la información que mencionamos, e incluso una miniatura de la imagen original.

Otros archivos, como documentos de texto, también incluye metadatos. Podrían indicar el tamaño del documento, quién es el autor, cuándo fue editado, y un resumen breve automatizado del contenido. Los datos EXIF y otros tipos de metadatos pueden ser extremadamente útiles para la verificación del contenido, además de para la creación y organización de catálogos.

Limpieza a fondo de los metadatos

En algunos casos puede que quieras eliminar metadatos de los archivos relacionados con violaciones de derechos humanos. Esto es particularmente relevante en casos donde compartir y publicitar evidencias de violaciones de derechos humanos, conlleva una amenaza para tu persona u otros involucrados en la documentación del incidente.

Se pueden usar distintas aplicaciones de software y herramientas en línea para 'limpiar a fondo' los metadatos de los archivos. Aunque no todos los metadatos se pueden eliminar —como el tamaño del archivo, las dimensiones de una imagen, o la hora de la última modificación— los metadatos relativos a quién creó y editó el archivo a menudo pueden ser eliminados. La eficiencia de las herramientas varía, así que lo mejor es probar con un par de ellas y comprobar que los metadatos son eliminados de forma efectiva.

Si está trabajando con un corresponsal de confianza, puede sugerirle que desactive los servicios de localización (datos GPS) en su dispositivo para ocultar su identidad. Practique la precaución cuando solicite imágenes, ya que el modelo de teléfono u otra información EXIF se podría usar para ubicar sus recursos.

La guía ***Security in a Box*** (algo así como Caja de Herramientas de Seguridad), del Tactical Technology Collective y Frontline Defenders, tiene aún más información sobre la eliminación de metadatos.

VERIFICA, VERIFICA, VERIFICA

Los datos de cualquier tipo —incluso de materiales que tú mismo has recopilado— requieren verificación exhaustiva para proteger tu reputación, y evitar que los operadores de campo de puedan sufrir daño. Es importante abordar cada pieza de contenido con un ojo crítico, aún cuando deseas que la pieza sea auténtica.

También tiene que aceptar que no hay un único método de garantizar la verificación. La verificación es un proceso para darte confianza a ti y a los demás de la veracidad del contenido. Debes ser tan transparente acerca de no sabes como lo eres sobre lo que si sabes, en beneficio de todos.

Cuando te encuentras en entornos bajo gran presión y con escasos recursos la verificación de datos digitales pasa a tener baja prioridad, en lugar de estar incorporada en los planes de investigación desde el principio. Si tienes dudas acerca de cómo verificar un tipo particular de contenido, es más seguro que consultes a expertos para que te ayuden.

Los cinco pasos de la verificación

1. **¿Cómo obtuvo el contenido?**
   Reflexione sobre los canales a través de los cuales viajó esa información antes de llegar a tu mesa ¿Cuántas veces cambió de manos?
2. **¿Quién creó el contenido?**
   ¿El contenido fue creado por la persona que lo compartió o subió en línea, o es alguien más? Pregunta si no lo sabes.
3. **¿De dónde viene el contenido?**
   Las descripciones y metadatos se pueden falsificar fácilmente. ¿Hay lugares conocidos a la vista o sonidos particulares (como sirenas de policía o dialectos) que puedan ayudarle a verificar la ubicación?
4. **¿Cuándo fue creado el contenido?**
   No puedes confiar en la información de fecha en un archivo. ¿Hay pistas visuales, como el clima por ejemplo? Una búsqueda inversa de la imagen puede mostrar si la foto aparece en alguna otra parte.
5. **¿Por qué fue creado el contenido?**
   ¿Puede determinar la motivación para compartir el contenido? ¿Qué intereses tiene quien lo subió?

¿Por qué verificar?

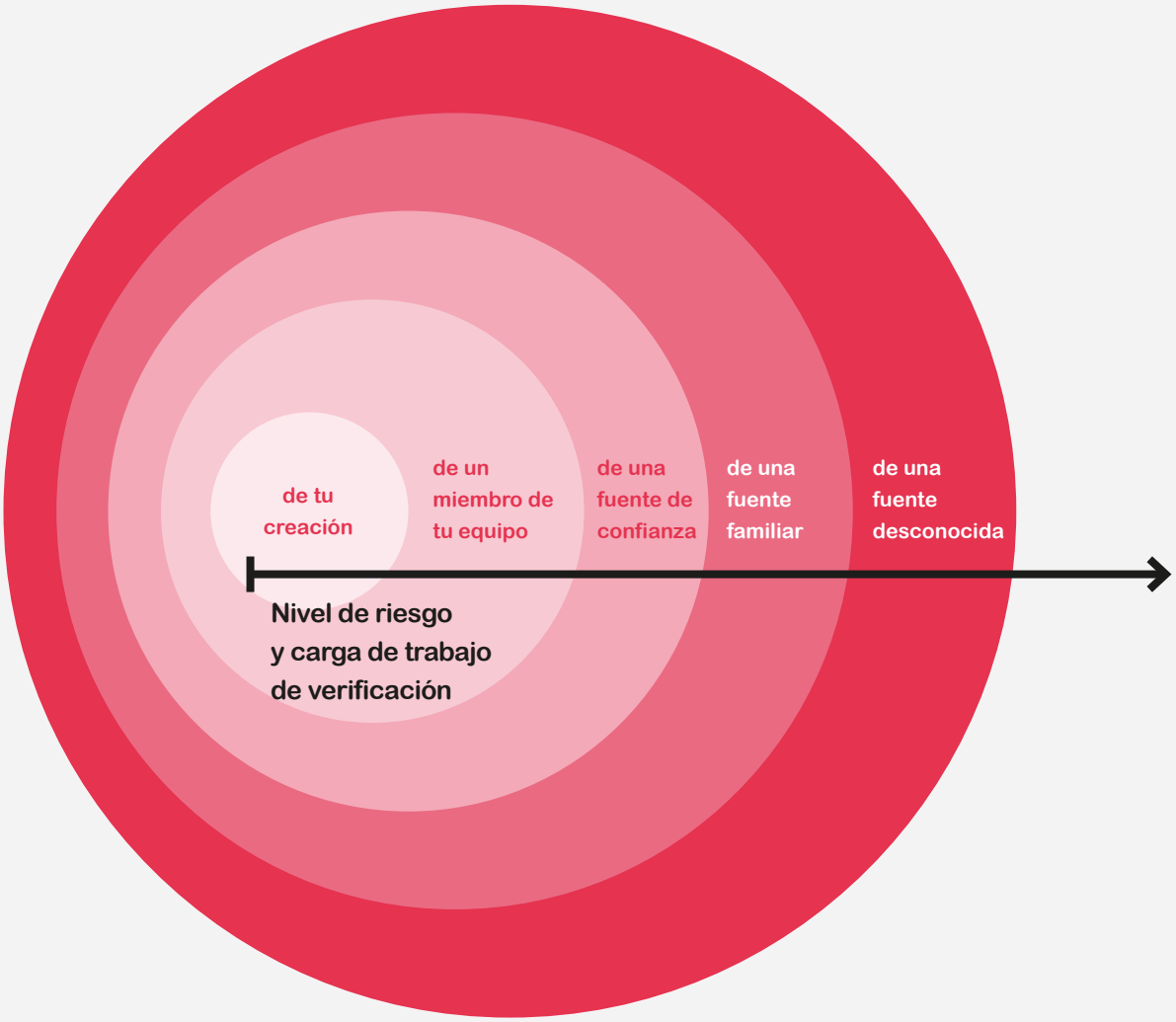
Puede parecer obvio, pero a menos que trabajes con material que hayas recogido tú mismo, o sean observaciones propias de primera mano, es importante verificar que la información con la que estás trabajando sea de hecho lo que pretende ser. Los riesgos de pérdida de reputación, además del riesgo que implica hacia los sujetos de la investigación requieren una apropiada diligencia al trabajar con nuevos datos de cualquier clase.

Pasos de la verificación

La verificación es un proceso evolutivo, y el producto final raramente es algo definitivo. Más bien es un proceso que brinda confianza a la información. Esta información puede pretender decirle algo acerca del quién, qué, dónde, y cuándo de un cierto evento. Hacerse esas mismas preguntas sobre la propia información es parte del proceso de verificación.

Pensar acerca de estas preguntas definirá qué herramientas precisa para iniciar una verificación del contenido:

¿CUÁL es la fuente?
¿QUIÉN subió o compartió el contenido?
¿DÓNDE fue creado el contenido?
¿CUÁNDO fue creado el contenido?
¿POR QUÉ fue creado el contenido?



Ejercicio

Verificar este vídeo de YouTube

Eres un investigador en derechos humanos, y necesitas verificar un vídeo de YouTube [*https://youtu.be/clrICxJihWI*] de uso excesivo de la fuerza por parte de la policía en una protesta en Río de Janeiro, Brasil, que un colega compartió contigo.

1. **Descarga el vídeo** para preservarlo, porque los contenidos sensibles en línea a menudo son eliminados.
2. Usando el *YouTube Data Viewer* (visor de datos de YouTube), **identifica la hora de publicación** (aunque no la hora de la grabación) que fue a las 5:30 pm (hora de Brasilia) del 14 de abril de 2014. Una búsqueda inversa de imagen sobre las miniaturas del vídeo no obtiene ninguna versión previa del vídeo en línea.
3. El creador listó convenientemente su nombre bajo el vídeo, y mirando en otras plataformas de medios sociales, deduces que **quien lo subió** parece ser un activista en Río de Janeiro.
4. El **vídeo y la descripción** son generosos en pistas acerca de la ubicación (Prefeitura do Rio). Para verificarlo, use el mapa en línea *Wikimapia* para buscar el ayuntamiento metropolitano de Río (prefeitura), y usas imágenes satelitales encontradas en Google Earth para cruzar referencias de elementos prominentes visibles (edificios de oficinas, puentes peatonales, etc.). Las fotografías con información de geolocalización de *Panoramio* (que se encuentran accesibles desde el mismo Google Earth) también coinciden.
5. La descripción dice que la protesta ocurrió un lunes por la mañana bajo un fuerte aguacero. Los *datos meteorológicos históricos* a los que se accediste mediante *WolframAlpha.com* son consistentes con lo que se veía en el vídeo (lluvioso y brumoso) haciendo por tanto parecer más creíbles al vídeo y **la presunta hora del día**.
6. Utilizas un reproductor de vídeo con con capacidad para reproducir en cámara lenta (en YouTube o mediante *VLC media player)* para observar más detenidamente **los uniformes e insignias** de la policía comparadas con las que muestran *los sitios web oficiales de la policía* [*https://www.facebook.com/gmrio.oficial*]. Anota los detalles para el caso de que puedan ser útiles para futuras investigaciones sobre los individuos implicados.
7. Finalmente, cuando buscas contenidos adicionales con el motor de búsqueda que utilizas regularmente, puedes encontrar **otros vídeos de la misma fecha y la misma protesta** [*https://youtu.be/sxyrP0yBBts*], que corroboran el vídeo.

Cómo verificar imágenes usando metadatos EXIF (Preguntas y Respuestas)

Todos y cada uno de los archivos de fotos digitales contienen información de metadatos llamada EXIF que puede identificar cuándo y dónde fue capturada una imagen. Esta información se añade al archivo en el momento en que la foto es tomada, sin importar el dispositivo que use. Los datos que brinda EXIF pueden ser muy útiles para verificación, pero también pueden ser manipulados cuando una imagen cambia de manos o ha circulado en un medio social.

¿Cuándo debo buscar metadatos EXIF?
Una imagen debe contener metadatos EXIF si viene directamente de la cámara de tu fuente a tu bandeja de entrada sin ser alterada o haber cambiado de manos. Si fue editada, todavía puede tener metadatos EXIF. Si una imagen no contiene metadatos EXIF, debe cuestionar su veracidad. Puede comprobar la existencia de metadatos EXIF y otros datos, y ver qué clase de cámara la creó o desde qué software fue exportada. Si ha sido alterada o manipulada, también puede contener otros tipos de metadatos.

¿Siempre habrá metadatos EXIF en tu imagen?
La mayoría de las plataformas de redes sociales despojan las fotos de metadatos EXIF o crean copias de baja calidad cuando una foto es subida a la plataforma (con la excepción de los sitios web dedicados a compartir fotos). Si estás verificando una foto proveniente de un medio social, habitualmente no encontrarás metadatos EXIF.

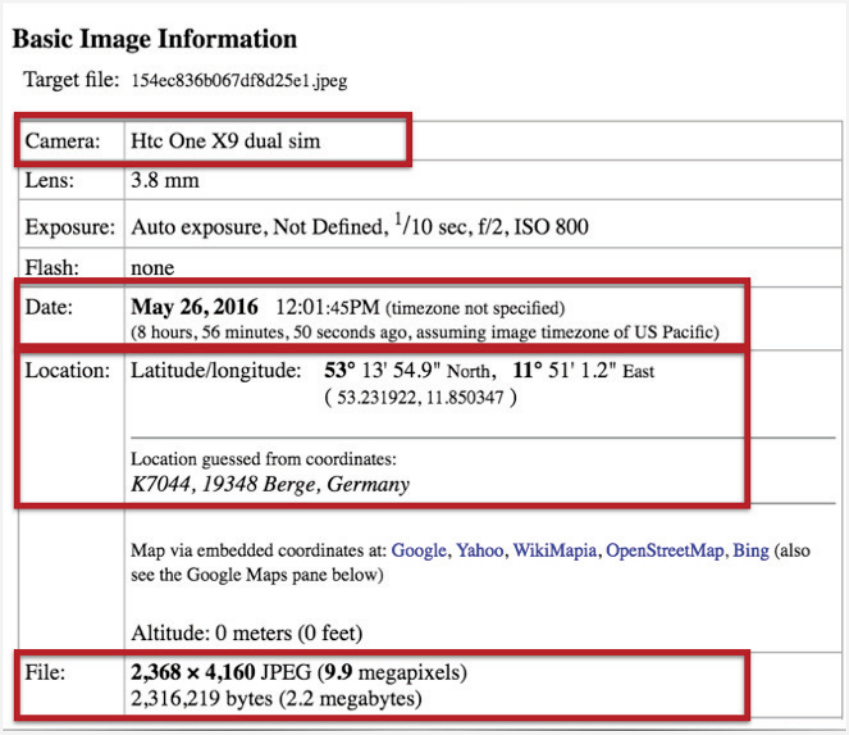
¿Cómo encuentro los metadatos EXIF?
Si buscas en línea "EXIF data viewer" (visor de datos EXIF) verás muchas opciones. Una de las herramientas más simples es Jeffry's EXIF Data Viewer [*http://regex.info/exif.cgi*] que también ofrece un complemento para varios navegadores web. También puedes encontrar los datos EXIF usando aplicaciones en tu computadora como Photoshop o iPhoto.

¿Se pueden manipular los metadatos EXIF?
Sí. Herramientas como *Geosetter* y otras aplicaciones de software de edición de fotos se pueden usar para falsificar los metadatos EXIF. Esto significa que los metadatos EXIF sólo se deben usar como uno de muchos pasos en el proceso de verificación. Herramientas como *JPEGSnoop* pueden detectar software que fue usado para manipular una imagen.

¿Qué pasa si alguien hace una foto de una foto antigua?
Los metadatos EXIF sólo pueden decirte el dispositivo que capturó la imagen, no saben nada acerca de lo que había realmente frente a la cámara. Incluso si los metadatos EXIF coinciden en fecha y ubicación, la imagen puede ser algo diferente de lo que pretende ser, por ejemplo, una foto de una foto.

En profundidad:

Qué dice una foto sobre tí...
Este es el aspecto que tienen los metadatos EXIF



Basic Image Information

Target file: 154ec836b067df8d25e1.jpeg

Camera:	Htc One X9 dual sim
Lens:	3.8 mm
Exposure:	Auto exposure, Not Defined, 1/10 sec, f/2, ISO 800
Flash:	none
Date:	**May 26, 2016** 12:01:45PM (timezone not specified) (8 hours, 56 minutes, 50 seconds ago, assuming image timezone of US Pacific)
Location:	Latitude/longitude: **53°** 13' 54.9" North, **11°** 51' 1.2" East (53.231922, 11.850347) Location guessed from coordinates: *K7044, 19348 Berge, Germany*
	Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 0 meters (0 feet)
File:	**2,368 × 4,160** JPEG (**9.9** megapixels) 2,316,219 bytes (2.2 megabytes)

1 2 3 4 5

Sólo algunos metadatos EXIF serán relevantes para la verificación.

1 **La cámara usada para capturar la imagen**

Este es el modelo de cámara o teléfono. Si, por ejemplo, intercambias correspondencia con una persona que ha compartido una imagen contigo, puedes corroborar lo que dicen los metadatos EXIF sobre la cámara usada para capturar la imagen con lo que la persona te dijo acerca del dispositivo con el que la capturó. Si te menciona un modelo de cámara o smartphone distinto del indicado en los datos EXIF, esto es una gran señal de alarma.

2 **La fecha y hora en que fue capturada la imagen**

This is important for checking the time a picture was captured, but EXIF does not indicate time zone. It can either reflect local time or Coordinated Universal Time (UTC), depending on device and settings. Some camera brands have their own metadata tags that supplement EXIF, and may include time zone data. There is also a non-standard EXIF tag for TimeZoneOffset, which can indicate the time offset relative to GMT. Many media upload sites, such as YouTube, default to Pacific Coast Time if the timezone is not embedded in the image. You should also consider if the time and date settings of the device could have been incorrect. This is more likely with a camera than a smartphone, which often auto-updates time and date settings.

3 **Coordenadas GPS del lugar donde fue capturada la imagen**

Si el dispositivo que captura la imagen tiene capacidades GPS (en su mayoría smartphones, aunque algunas cámaras también las tienen), y la persona que ha capturado la imagen ha activado estas capacidades, los metadatos EXIF pueden mostrar las coordenadas GPS del lugar donde fue tomada. GPS significa Global Positioning System (sistema de posicionamiento global) —un sistema de localización satelital. Si están disponibles, la mayoría de los visores de metadatos EXIF mostrarán estas coordenadas en un servicio de mapas en línea.

4 **Las dimensiones en píxeles de la imagen**

Las dimensiones en píxeles de la imagen (ancho y alto) son útiles de dos maneras. Primero, dos cámaras con la misma capacidad en megapíxeles pueden producir imágenes con distintas dimensiones. Por ejemplo, las cámaras Fujifilm XT-2 y Leica M-D Typ 262 ambas producen imágenes de 24 megapíxeles, pero con distintas dimensiones. Las dimensiones en píxeles de la Fujifilm XT-2 son: 6000 x 4000 píxeles, en cambio las dimensiones en píxeles de la Leica M-D Typ 262 son 5976 x 3992 píxeles.

Las dimensiones en píxeles también pueden proporcionar pistas de si una imagen ha sido recortada. Como regla general, la anchura y altura de una imagen deben resultar en un número entero al dividirlas entre ocho. Las resoluciones de la mayoría de las cámaras digitales son múltiplos de ocho, lo que se puede verificar revisando las especificaciones técnicas de una cámara (hay excepciones a esta regla, especialmente con las aplicaciones móviles y las funciones panorámicas).

5 **El recuento de píxeles de la imagen**

Cada cámara hace tomas con distintos tamaños de imagen. Por ejemplo, un iPhone 5 produce una imagen de 8 megapíxeles, mientras que un Samsung Galaxy S5 produce una imagen de 16 megapíxeles. En la figura anterior, vemos que la imagen es de 9,9 megapíxeles, es decir, 2368 x 4160 píxeles (un megapíxel = un millón de píxeles). Si el recuento de píxeles y las dimensiones no coinciden con los tamaños soportados por el presunto dispositivo, debería ponerse en alerta y hacer preguntas a tu contribuidor.

Usar búsquedas inversas de imagen para verificar e identificar

Los motores de búsqueda de imágenes son grandes herramientas para la verificación e identificación. Cuando subes una foto a un motor de búsqueda de imágenes y realiza una "búsqueda inversa de imagen", el motor compara nombres de archivo coincidentes e imágenes similares que ya aparecen en línea. Esto puede ayudarte a determinar si una foto es lo que crees que es, si es más antigua de lo que crees, o si ha sido usada previamente en un contexto o país distinto.

1. **Encuentra el motor de búsqueda adecuado para ti.** *TinEye* y *Google Image Search* ofrecen las bases de datos más exhaustivas. Pero muchos otros motores de búsqueda (Bing, Yandex, Baidu) también ofrecen búsqueda inversa de imágenes. Pruebe a ver cuál te funciona mejor.
2. **Realiza siempre dos búsquedas**
   Cada motor de búsqueda inversa de imagen consulta una base de datos distinta, e indexa nuevas imágenes a diferente velocidad. Tu imagen puede aparecer en un motor de búsqueda a la vez que no aparecer en otro.
3. **Ordena los resultados por antigüedad.**
   Con el más antiguo primero, si la imagen es de un evento distinto del declarado, la discrepancia se revelará rápidamente.
4. **Localiza referencias geográficamente.**
   Si tratas de identificar elementos prominentes en una imagen o vídeo, un motor que permite búsquedas "similar a" es de gran ayuda, ya que los lugares públicos están muy documentados.

¡Cuidado! La búsqueda inversa de una imagen no puede decirte cuándo fue tomada una imagen. Únicamente puede decirte si una imagen ha sido indexada previamente en la Web, y cuándo.

¡Cuidado! Si tu imagen no aparece en una búsqueda inversa de imagen, no significa que sea nueva u original. La imagen podría haber estado almacenada en un disco duro por años.

Caso de estudio

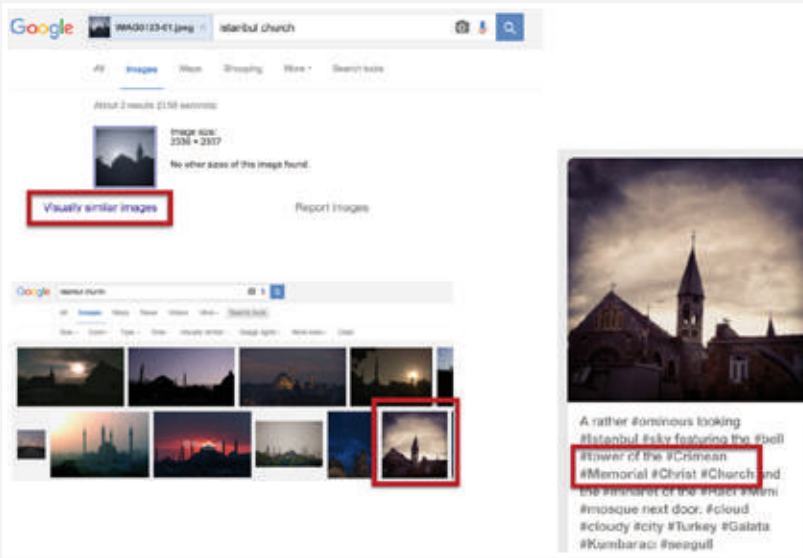
Verificar la localización de esta imagen

Tenemos una foto de una iglesia que se dice que está en Estambul, Turquía.

Para verificar este elemento prominente mediante búsqueda inversa de imagen, subimos la imagen a Google Images y escribimos “Istanbul church” (o “iglesia Estambul”) a continuación de la imagen.

Tenemos la opción de buscar por “imágenes visualmente similares”, lo que nos lleva a una página donde una imagen tiene las mismas torre y tejados. Haciendo clic en esa imagen sugiere que es la Iglesia Cristiana Memorial de Crimea en Gálata, Turquía, que ahora podemos situar en un mapa.

También puedes hacer este tipo de verificación con vídeos. Simplemente haz una captura de algún elemento prominente del vídeo, y sigue los mismos pasos.



DATOS DE REDES SOCIALES

En junio de 2014, un vídeo de una ejecución extrajudicial en República Centro Africana fue publicado en línea por un periódico, y fue ampliamente compartido a través de las redes sociales. Sin embargo, tras verificarlo, Amnistía Internacional descubrió que el incidente tuvo lugar realmente en Nigeria, y el vídeo terminó siendo la base de la investigación de Amnistía ***implicando a militares de Nigeria en crímenes de guerra***.

Este ejemplo muestra las enormes trampas y oportunidades del contenido en las redes sociales para la investigación en derechos humanos. Sea texto, fotos, vídeo o audio, tiene el potencial de desvelar atrocidades ocultas, mientras al mismo tiempo pone en peligro la reputación de una organización si se usa de forma descuidada. Además, la gran cantidad de contenido compartido entre múltiples plataformas puede abrumar fácilmente a los investigadores, e incluso suponer la necesidad de desarrollar destrezas especializadas en organización y rastreo.

Las redes sociales son muy diferente a las fuentes de información tradicionales, como testigos presenciales o información periodística, no solo porque el origen de la información es generalmente poco claro y debido a que la ***desinformación se propaga*** en forma increíblemente rápida desde una persona a miles. Pero al mismo tiempo, las redes sociales se están volviendo cada vez más importantes. Incluso los gobiernos y los militares usan canales en línea (a veces en exclusiva) para distribuir información de modo directo al público.

Ejemplos recientes incluyen la cobertura informativa continua por parte de los militares rusos de sus ***operaciones militares*** sobre Siria en YouTube, y las emisiones en línea de las ***Fuerzas de Defensa Israelíes*** acerca de sus operaciones sobre Gaza en 2014.

Un par de ejemplos pueden ayudar a ilustrar las enormes oportunidades para la reconstrucción de eventos e investigaciones a largo plazo. En ***Egipto***, el contenido de las redes sociales permitió la reconstrucción del asesinato de un manifestante pacífico por parte de la policía en 2015, y subsecuentemente forzó una investigación y un juicio. En ***Nigeria***, los contenidos las redes sociales jugaron un papel crucial para documentar crímenes de guerra en 2014.

Cuando los investigadores adquieren destreza en formular preguntas adaptadas a las redes sociales y empleen herramientas técnicas para procesar conjuntos más grandes de datos, podrán efectuar análisis avanzados que abarquen períodos de tiempo más largos, en diferentes lugares y en múltiples idiomas. En 2016, Abodo, un sitio de ofertas de alquiler de alojamiento en línea, ***analizó millones de twits*** para ver cómo el uso de lenguaje despectivo sobre raza, etnicidad, género, religión y orientación sexual, variaban en distintas partes de los Estados Unidos. En 2014, Global Voices efectuó ***un "análisis de sentimiento" de twits rusos*** sobre la amenaza de guerra en Crimea, mostrando una oposición leve.

Iniciarse con la investigación en medios sociales

Utiliza las redes sociales para la defensa de los derechos humanos siempre de forma segura, ética, y significativa. Necesitas descubrir, organizar, preservar y verificar. El propósito de las siguientes preguntas es proporcionar orientación. Úsalas en tu investigación, al margen de con qué plataformas te encuentres trabajando.

¿Qué plataformas y aplicaciones son dominantes en tu país o región?

"Red Social" es un término amplio, y las preferencias por aplicaciones de los usuarios varían entre países y regiones. Mientras Twitter puede ser popular en los Estados Unidos, la gente en Egipto o Burundi puede preferir usar Facebook. Reconocer estas diferencias es crucial al rastrear incidentes de derechos humanos.

¿Qué palabras clave y hashtags se usan para compartir contenido sobre tu tema?

La gente se comunica usando palabras clave específicas o hashtags. Sigue estos identificadores para descubrir contenido. Ej., los usuarios en Burundi usaron #1212massacre para describir la violencia de diciembre de 2015. Además, el lenguaje usado por los testigos puede ser más emotivos, con mayor sentimiento de lo que encontrarás con la primera búsqueda que se te ocurra.

¿Puede acotar su búsqueda y filtrar los resultados?

Algunas plataformas de redes sociales permiten buscar por ubicación, fecha, o tipo de contenido. Por ejemplo, ***Tweetdeck***, una herramienta para gestionar Twitter, le permite buscar sólo imágenes y vídeo, a la vez que excluye retwits. También puede crear ***listas*** de usuarios de confianza para seguir contenido de forma selectiva.

Foto: Ejemplos del tipo de palabras usadas en las redes sociales en situaciones de noticias de impacto, incluyendo "I" (yo) y "my" (mi), lo que podría ayudarle a buscar testigos presenciales.
Fuente: Deutsche Welle/Reveal Project

¿Has guardado el contenido que estás revisando?
El contenido en línea puede desaparecer muy rápidamente, eliminado por quien lo subió o por la red social que lo aloja. Haz capturas de los mensajes o descarga las imágenes. Para los vídeos, existen herramientas como ***VideoVault***.

¿Puedes verificar la información?
Los mensajes en las redes sociales han de ser examinados cuidadosamente por determinar su precisión. La tentación de usar sin criterio crítico contenidos visuales ampliamente compartidos puede ser más grande que cuando se trata de declaraciones de testigos presenciales, pero en ambos casos se debe aplicar el mismo criterio de verificación.

¿Tienes otras fuentes de información para corroborar?
No confíes en un único mensaje en una red social cuando sea probable que otros mensajes, vídeos y fotos en línea haga referencia el mismo incidente. Combinar distintas piezas de información e incluir testimonios de testigos presenciales y reportajes de noticias, te ayudará a construir un caso mucho más fuerte.

¿Hay riesgos de privacidad o consideraciones éticas?
Como con cualquier fuente, considera los riesgos potenciales para los individuos si compartes o publicas sus palabras o imágenes. Además, pregúntate a tí mismo si puedes estar haciendo daño de forma no intencionada a las comunidades afectadas por un conflicto.

En profundidad

Primum non nocere

El principio primum non nocere (primero no hacer daño, DNH o Do-Not-Harm) es un marco útil a tener en cuenta en el contexto de la transformación pacífica de conflictos (armados o de otra índole). Este principio requiere plantear cuestiones acerca de si las intervenciones contribuyen a la **unificación** o a generar **separación** adicional.

Compartir imágenes o vídeos con fuerte carga sobre abusos de derechos humanos o atrocidades vía medios sociales podría profundizar las divisiones entre ambos bandos en un conflicto, dependiendo de cómo sean presentadas. Si se difunde material falsificado afirmando mostrar atrocidades, podría incluso intensificarse el conflicto. Esto plantea serias controversias éticas sobre compartir contenido de redes sociales, y resalta la importancia máxima de la verificación y la presentación ponderada de datos con miras a extinguir en lugar de perpetuar la violencia.

Para más detalles sobre el principio primum non nocere vea *Anderson, Mary B: "Do No Harm: How Aid Can Support Peace – Or War" Boulder, CO: Lynne Rienner Publishers, 1999*.

Foto: "***Non-Violence***", UN Foto/Michos Tzovaras (CC-BY-NC-ND 2.0)

Tres categorías de “fake” (falsificación) de las que cuidarse en las redes sociales

Atribución errónea

Esta es, por demás, el desafío más prominente en la investigación en derechos humanos.
Los contenidos son reciclados en línea continuamente, y se comparten con fecha, ubicación o atribución erróneas.

Ejemplo
Un vídeo altamente gráfico fue compartido durante la violencia post-electoral en Costa de Marfil en 2011. Sin embargo, el vídeo tenía ***varios años***, y ya había sido compartido en múltiples países.
Una técnica simple para detectar contenido antiguo es hacer una ***búsqueda inversa de imagen***.
Esto también puede hacerse con la imagen de bajada o la miniatura de un vídeo. (Revisa el capítulo de verificación de esta guía).

Escenificación

Una situación, un evento o los detalles específicos de un incidente pueden ser escenificados.
Por ejemplo, un grupo armado en Siria posó en un vídeo de YouTube con lo ***que terminaron siendo pistolas de juguete***.

Ejemplo
El “Syria Hero Boy Video” (vídeo del chico héroe de Siria) fue un ***vídeo escenificado***, producido por un cineasta noruego.
Es un ejemplo de libro de cómo mirando la fuente y el rastro digital de la persona que lo subió originalmente, deberían plantearse dudas. El canal de YouTube que ***alojó el vídeo por primera vez*** era nuevo y sólo contenía este vídeo altamente dramático—un signo de alerta.

Distorsión técnica

ebes ser consciente de la facilidad cada vez mayor con la que el contenido puede ser manipulado.
En especial, una imágen puede ser falsificada por medio de recortes, borrado de detalles o composición con otras imágenes para representar eventos falsos.

Ejemplo
En 2013, las autoridades de la provincia de Anhui, China, publicaron una foto trucada que mostraba a un vice-alcalde “***sobrevolando como un fantasma a una señora mayor del tamaño de una marioneta***”. Tras muchas burlas en línea, admitieron que había sido el resultado de dos fotos fundidas y expresaron su “profundo pesar”.

DATOS QUE SE SOSTENDRÁN EN UN TRIBUNAL

Pruebas legalmente admisibles

La documentación de situaciones de derechos humanos tiene un potente impacto sobre los procedimientos legales. El Tribunal Penal Internacional, además de varios otros tribunales híbridos, busca activamente el apoyo de la sociedad civil. Pero los tribunales son lentos en adoptar nuevas tecnologías, y los jueces, que tienden a ser de avanzada edad, a menudo no están familiarizados con la manera en que los datos digitales pueden adaptarse a las normas probatorias comunes. Variará entre jurisdicciones si un vídeo de YouTube será aceptado como evidencia legal.

Por ejemplo, en 2015, el sistema de justicia de Suecia ***procesó a un ex-combatiente en Siria*** por tortura, en base a un vídeo publicado en Facebook. Muchos sirios están reuniendo colectivamente tales contenidos en línea para acusar en otros países a antiguos funcionarios, militares, y combatientes que hayan abandonado el país.

Requisitos para el tribunal

Si quieres que tus datos gitales deriven en acusaciones criminales, necesitas asegurarte de registrar todos los metadatos relevantes. Un tribunal debe poder identificar claramente la localización de un vídeo, bien mediante coordenadas de posición incrustadas en el vídeo, o elementos prominentes que se puedan identificar en el contenido del vídeo. Además, el objeto del vídeo se debe ver con claridad — vídeos borrosos o movidos que arrojen dudas acerca de quién está en la grabación o qué actos están cometiendo, probablemente no serán aceptados.

Considera además la cadena de custodia. Para que sean aceptadas para una acusación criminal, la mayoría de tribunales necesitan conocer cada individuo que manipuló el contenido, comenzando por el creador original y terminando por la fiscal en el tribunal. La cadena de custodia debe mostrar exactamente quién tuvo posesión del contenido para salvaguardarlo de la manipulación de la evidencia, cuándo, y durante cuánto tiempo. Cuanto más cerca estés de acceder a la grabación original, más fácil será presentarlo en el tribunal porque la cadena de custodia será más corta y más fácil de probar.

También será importante que trabajes imparcialmente y minimices cualquier posible alteración de los datos. Un abogado defensor podría argumentar que los datos han sido corrompidos, son tendenciosos e intentará poner en duda la motivación de los mismos. Necesitarás llevar a cabo al menos algún análisis para conseguir que la documentación pueda ser encontrada y hacerla comprensible, pero trata de mantener este análisis al mínimo posible.

Riesgos de tomar parte en los tribunales

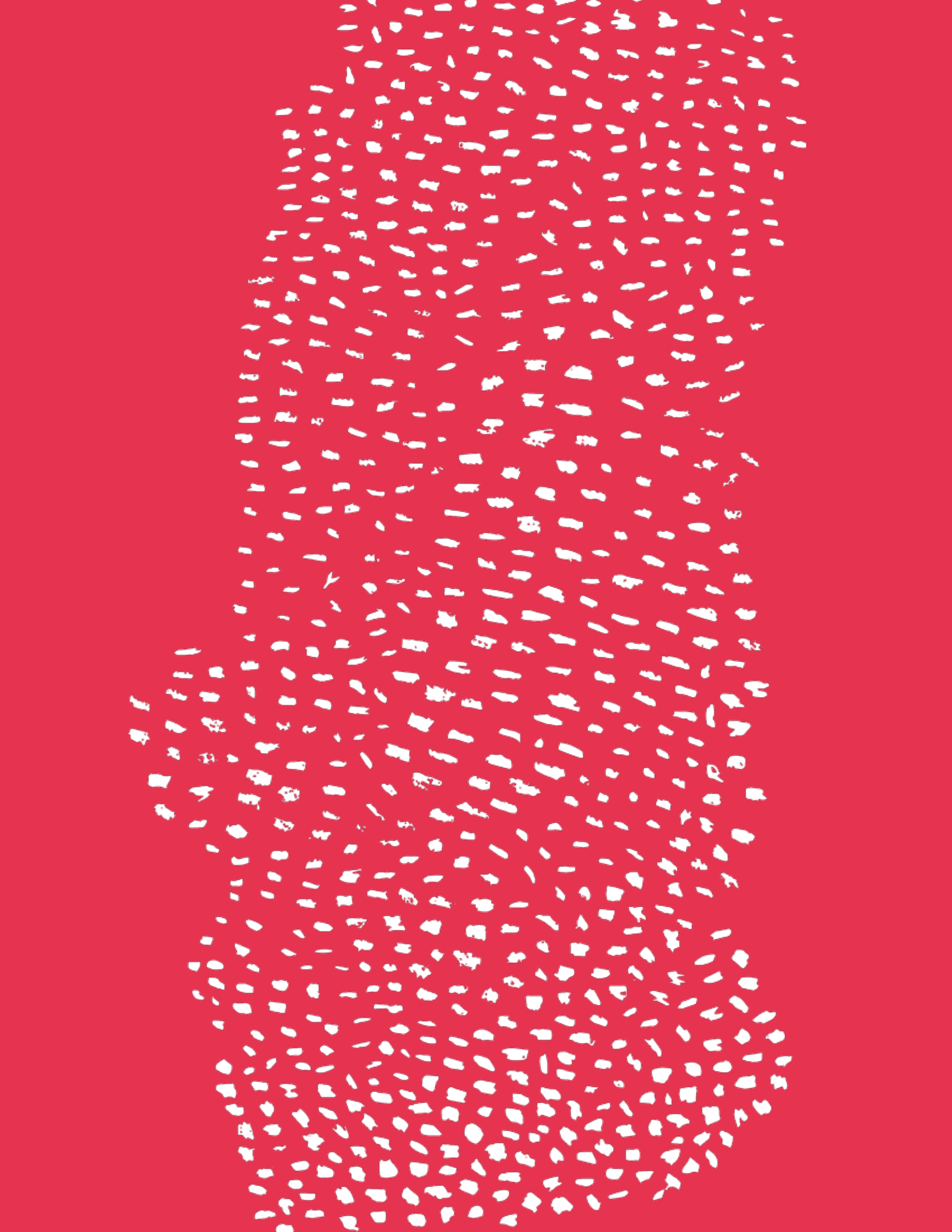
Al tomar parte en los procesos de justicia, las organizaciones de derechos humanos se arriesgan a recibir citaciones judiciales para divulgar evidencias confidenciales, como nombres y fechas, en un tribunal abierto durante el procedimiento previo al enjuiciamiento que habilita a cada parte a acceder a las evidencias de las demás ("principio de publicidad" o "rules of discovery").

Si estás trabajando con la fiscalía, intenta establecer un sistema de protección de testigos. Muchos procedimientos judiciales son públicos, y todas tus precauciones podrían venirse abajo instantáneamente si el testigo declara y su nombre e información personal se hacen públicos. Evita entablar juicio en tribunales que no protegen a los testigos, para que los tuyos no sean dañados como resultado de su testimonio.

Otras formas de justicia

Si estos riesgos son apabullantes, no está todo perdido. ***The Syria Justice and Accountability Centre***, (centro para la justicia y la rendición de cuentas en Siria), una organización que documenta violaciones de los derechos humanos y de las leyes humanitarias internacionales en el conflicto sirio, ha recopilado más de un millón de piezas de datos durante cinco años. La mayoría de la documentación —quizá hasta el 90 por ciento— probablemente no será aceptada en un tribunal, pero toda la documentación restante se puede usar para otros tipos de procesos de justicia transicional.

La justicia transicional incluye comisiones de la verdad, conmemoraciones, programas de reparación y reformas institucionales, todo lo cual se puede usar para ayudar a sanar y compensar heridas pasadas, y caminar hacia la reconciliación. En el caso de las reformas institucionales, grandes conjuntos de datos pueden mostrar tendencias abusivas y corruptas en el sector judicial de un país. Estos datos pueden ayudarte a evidenciar aspectos del sector que requieren ser reformados, y pueden guiar un proceso de examen y reforma legal del país. Reformando el sector de la justicia, un país puede avanzar hacia el afianzamiento de un sistema que evite que la situación se repita.



Técnicas prácticas

ESTADÍSTICAS DE GOBIERNO ABIERTO

Los gobiernos recopilan datos para toma de decisiones y planificación informadas. Hay una presión para que los gobiernos abran sus datos al público como modo de incrementar la transparencia, la rendición de cuentas y la participación ciudadana. Ejemplos de iniciativas de datos abiertos están en auge por todo el mundo, incluyendo portales en línea y aplicaciones para que los ciudadanos accedan a datos relevantes del gobierno para su propio uso. Estos recursos pueden proporcionar una abundancia de información para los investigadores en derechos humanos, pero también plantea desafíos.

Acceder a datos del gobierno

Una gran cantidad de datos secundarios son públicamente accesibles en sitios web de oficinas nacionales de estadística. Adicionalmente, muchas agencias publican en línea evaluaciones de programas del gobierno.

Donde los datos no estén disponibles en línea, tal vez pueda entregar una solicitud en base a la libertad de información. Más de 95 países reconocen un derecho general de acceso a la información del gobierno, con excepciones para la información considerada demasiado sensible para compartir. Más información en: ***http://right2info.org/***.

Descargar, almacenar y organizar datos del gobierno

Los datos gubernamentales a menudo se presentan en formato PDF, haciendo de la búsqueda y análisis de datos un desafío. The School of Data tiene tutoriales sobre cómo extraer datos de un PDF, de forma que pueda trabajar en un formato amable y familiar como CSV o XLSX.

Tipos de datos del gobierno

Tipo de datos	Ejemplos	Pros	Contras
Registros administrativos Creados cuando agencias del gobierno e instituciones interactúan con el público. También pueden incluir datos de transacciones con proveedores de servicios y financieros.	Estadísticas vitales sobre poblaciones, como tasas de muertes y nacimientos; estadísticas de empleo y desempleo. Beneficiarios de políticas y servicios sociales. Contratos con proveedores y contabilidad.	Donde los registros administrativos se actualicen con frecuencia, puede ser un recurso simple, rastreable y cuantitativo que puede mejorar la transparencia y ayudar a erradicar la corrupción.	Sólo se realizan para quienes usan determinados servicios públicos, así que la cobertura no siempre es fiable. Ej., las estadísticas de crímenes pueden infra-representar asaltos sexuales, algo en extremo no denunciado.
Sondeos estadísticos También llamados sondeos de muestras, sólo recopilan datos de un subconjunto de la población, con el objetivo de extraer inferencias para toda la población.	Sondeos demográficos de salud, sondeos de fuerza laboral, sondeos de ingresos y gastos de núcleos familiares.	Los sondeos pueden ser una forma, eficiente en coste para los gobiernos, de recopilar información donde los datos de fuentes administrativas no estén disponibles.	Cualquier prejuicio en la selección de la muestra puede llevar a que el sondeo no sea representativo de la población en conjunto.
Censos Catálogo de todos los miembros de un país o territorio.	Habitualmente los países realizan censos de población, viviendas, agricultura y establecimientos industriales.	Proporcionan datos básicos sobre características clave de la población y sobre variables que no cambian con rapidez.	Los censos de población se realizan habitualmente a intervalos de diez años por su complejidad y coste.

Evaluar la fiabilidad de los datos del gobierno

Los datos del gobierno no siempre son precisos. No es infrecuente que las bases de datos gubernamentales y no gubernamentales contengan información contradictoria. Distintos métodos de recopilación de datos, análisis y cómputo, son las causas principales de tales conflictos.

Concepto	Definición	Problemas potenciales
Validez	Los datos deben reflejar lo que tratan de medir (ej., el ejercicio de un derecho) de la forma más fiel y precisa posible.	La mayoría de datos secundarios se recogen para usos distintos del monitoreo de derechos humanos. Se debe cambiar su propósito, y esto puede ser un desafío.
Fiabilidad	Se refiere a la consistencia o fiabilidad de los datos. En otras palabras, datos recopilados varias veces de la misma manera deberían producir resultados similares.	Ambigüedades o desviaciones en la forma de recopilar los datos (ej., en la forma de elaborar las preguntas del sondeo, o de tomar muestras una población) podrían hacer no fiables los datos.
Imparcialidad	Los datos se deben recoger de forma que se respete la independencia científica, y de manera objetiva, profesional y transparente.	Una oficina estadística nacional que no sea independiente puede "tornar" los números de forma que una situación parezca mejor de lo que realmente es.

Para evaluar la validez, fiabilidad e imparcialidad de los datos, pregúntese:

- **¿Cuál es el objeto de los datos?**
  Para algunos asuntos particularmente sensibles o controvertidos, los datos del gobierno pueden ser notoriamente no fiables.
- **¿Cómo se formulan las preguntas?**
  A veces las preguntas son tendenciosas, y por tanto predisponen la respuesta.
- **¿Cuál es el tamaño de la muestra?**
  Puede ser demasiado pequeña para ser representativa.
- **¿Cada cuánto se recogen los datos?**
  Los datos pueden resultar caducos.
- **¿Quién recopila los datos?**
  Puede haber un conflicto potencial de intereses o limitación de recursos.
- **¿Quién publica los datos?**
  Puede haber un conflicto potencial de intereses.

Analizando estadísticas desde la perspectiva de derechos humanos

Cuando los datos del gobierno se combinan y se analizan en comparación contra los estándares y principios de los derechos humanos, pueden resultar útiles para hacer evidentes las violaciones de derechos económicos sociales y culturales. Al mirar estadísticas del gobierno es útil, por tanto, que te preguntes: ¿Qué me dice esto acerca de la disponibilidad, accesibilidad y calidad de los bienes y servicios? ¿Hay regiones o grupos concretos que están marginados o contra los que se discrimina? ¿Cómo han cambiado las cosas con el tiempo? ¿Han mejorado o empeorado?

Caso de estudio

Datos del gobierno como evidencia de discriminación sistemática en Guatemala

En 2009, el Center for Economic and Social Rights (CESR) y el Instituto Centroamericano de Estudios Fiscales publicaron un informe sobre el derecho a la salud materna en Guatemala que mostró pruebas de discriminación contra las mujeres indígenas.

Basándose en datos del Banco Mundial, del Programa de Naciones Unidas para el Desarrollo y de las oficinas nacionales de estadística, citaron sondeos demográficos de salud que mostraban que Guatemala obtuvo resultados de mortalidad materna ubicados entre los peores y los más inequitativos de América Latina. Las mujeres indígenas tenían tres veces más posibilidades de morir durante el parto o el embarazo que las no indígenas, y más del 50% de las muertes podrían haber sido evitadas con cuidados especializados. Las estadísticas administrativas mostraron serios problemas con la disponibilidad y calidad de los servicios.

La pobre implementación de políticas pudo relacionarse con la inadecuada inversión de recursos en el sector sanitario. Las asignaciones al sistema sanitario han permanecido en torno al 1% del PIB desde el final de la guerra en 1996, por debajo de las de los países más pobres de América Central. La distribución del gasto per cápita en salud también fue altamente inequitativa, con tres veces más dinero asignado a la capital que a Quiché, la región más pobre. La baja inversión social estuvo directamente vinculado a la baja base impositiva del país, que se generó mayoritariamente mediante impuestos indirectos regresivos que incidieron en los pobres de forma desproporcionada, mientras los sectores de negocios del país disfrutaron de privilegios e incentivos fiscales.

Todas estas cifras se combinan para conformar la fundada conclusión de que Guatemala no estuvo haciendo todo lo que razonablemente pudo para mejorar la salud materna, discriminando en efecto contra las mujeres indígenas más pobres. Vea el informe completo aquí: ***http://www.cesr.org/section.php?id=33***.

Foto: ***Street Scene, Chajul, Quiché*** en Guatemala (2014) por Adam Jones en flickr (CC-BY-SA 2.0)

DATOS DE PRESUPUESTOS PARA DERECHOS HUMANOS

Al establecer prioridades presupuestarias, los gobiernos pueden, de forma involuntaria o deliberada, desatender los estándares de derechos humanos. Por ejemplo, los recortes presupuestarios para el sistema de justicia criminal pueden dejar a los acusados con bajos ingresos en detención provisional durante largos períodos más allá de lo razonable. Una decisión de reducir los subsidios o incrementar impuestos sobre determinados productos domésticos o de higiene, de modo indirecto, puede ser discriminatoria contra las mujeres. La competencia en el análisis de datos presupuestarios puede, por tanto, ser un componente esencial de la investigación integral en derechos humanos, especialmente ahora que hay tantos datos disponibles en línea.

Tipos de datos presupuestarios

Puede ser útil dividir un presupuesto en tres partes principales: cómo se generan los ingresos, cómo se asignan los presupuestos, y cómo se efectúan en realidad los gastos.

Datos sobre ingresos presupuestarios

¿Están generando *suficientes* recursos las políticas fiscales? ¿Lo hacen *equitativamente*?

Entre los datos útiles para juzgar la suficiencia de recursos se incluyen:

- Ingresos del gobierno en porcentaje del PIB.
- Ingresos por impuestos en porcentaje de los ingresos del gobierno.
- Esfuerzo fiscal (relación entre recaudación real y capacidad impositiva; eficiencia recaudatoria).
- Volumen de flujos financieros ilícitos.
- Ingresos por impuestos en porcentaje de los ingresos totales.

Entre los datos útiles para juzgar la equidad de los recursos se incluyen:

- La composición de los impuestos (ej. porcentaje que constituyen los impuestos sobre el ingresos, impuestos a los bienes y servicios, impuestos al sector corporativo, etc.).
- Impuestos pagados por distintos grupos en porcentaje del total de sus ingresos.
- Exenciones concedidas.

Caso de estudio

Dinero por el desagüe

Un país asigna el 1,5% de su presupuesto al sector de saneamiento. Esta asignación ha decrecido durante los últimos diez años. El 75% del dinero que se asigna al sector de saneamiento subsidia el saneamiento de la red de aguas (tuberías de alcantarillado y de aguas servidas o cloacales), pero los núcleos familiares pobres en asentamientos informales se valen del saneamiento in-situ (ej. letrinas, pozos negros). ¿Hace esto saltar las alarmas desde la perspectiva de los derechos humanos? El gobierno podría estar de hecho discriminando a los núcleos familiares en asentamientos informales.

The International Budget Partnership tiene una serie de recursos que explican cómo algunos estándares internacionales de derechos humanos, tales como la realización progresiva de reformas (progressive realisation), la no discriminación (non-discrimination) y el máximo aprovechamiento de los recursos disponibles (maximum available resources) pueden ayudar a responder esta pregunta: ***http://www.internationalbudget.org/publications/escrarticle2/***.

En profundidad

¿Qué es un presupuesto de género?

El presupuesto de género es un tipo concreto de análisis presupuestario usado para evaluar el impacto del gasto del gobierno en mujeres, hombres, chicas y chicos. Por ejemplo, en el área de la salud, hombres y mujeres tienen necesidades similares en lo que respecta a la gripe y la malaria. Sin embargo, las mujeres tienen mayores necesidades que los hombres en términos de salud reproductiva.

El presupuesto de género es una forma nueva y en evolución de visualizar y afrontar los efectos discriminatorios de decisiones sobre recursos. Hay herramientas útiles disponibles en: ***www.gender-budgets.org***.

Foto: ***Unidad de Salud Primaria de San Malen en Pujehn, distrito de Bo, Sierra Leona*** (2013), por H6 Partners en Flickr (CC-BY-NC-ND 2.0)

Datos sobre asignación presupuestaria

Los siguientes pasos pueden determinar si las asignaciones presupuestarias están en línea con los estándares y principios de los derechos humanos.

1. **Calcular**
   - *Relaciones o cuotas* (porcentaje de algo sobre el total)
   - *Promedios* (valores medios de las asignaciones presupuestarias)
   - *Gasto por unidad o per cápita* (valor por persona)
2. **Realizar comparaciones** (identificar áreas y grupos de prioridad)
3. **Analizar tendencias** (comparar en el tiempo progresiones ajustadas a la inflación))

Datos sobre el gasto del presupuesto

A menudo, lo que los gobiernos planean gastar y lo que gastan realmente es distinto. La corrupción es la causa principal, pero los sistemas ineficientes de administración financiera, los desvíos de fondos y una débil supervisión, también pueden contribuir a la brecha.

Existen diferentes herramientas y métodos (a menudo llamados aproximaciones "seguir el dinero") que rastrean datos de gastos, incluyendo: la supervisión del gobierno y los informes de auditoría, monitorear el proceso de adjudicación pública, y la supervisión y auditoría no gubernamental del gasto.

Acceder a los datos presupuestarios

Los presupuestos son documentos oficiales del gobierno. En general, deben estar disponibles desde el sitio web del tesoro público o el ministerio de finanzas, las oficinas del auditor general, o las agencias anticorrupción. Sin embargo, en muchos países los documentos relevantes no se hacen públicos, y pocos gobiernos ofrecen mecanismos apropiados de participación pública en los procesos presupuestarios.

Para conocer hasta qué punto es abierto el proceso presupuestario de tu gobierno, visita el ***Open Budget Index*** (índice de apertura presupuestaria) que clasifica los países de acuerdo con el grado al que el público puede acceder a ocho documentos clave en el proceso presupuestario (***http://internationalbudget.org/what-we-do/open-budget-survey/***)

Otras fuentes relevantes de datos para analizar presupuestos vienen de las instituciones financieras internacionales, como el Banco Mundial y el Fondo Monetario Internacional. Las ONGs que trabajan contra la corrupción también pueden ayudar a localizar datos presupuestarios.

Dependiendo de la región donde te encuentras y el contexto político, puede ser juicioso usar una VPN u otra herramienta de anonimización, para enmascarar sus búsquedas de datos presupuestarios.

Caso de estudio

Recortes discriminatorios de presupuesto en España

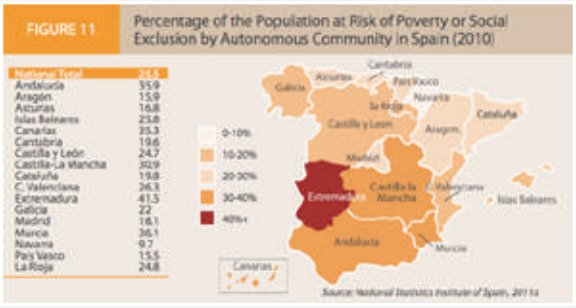
Un estudio de 2012 efectuado por el Center for Economic and Social Rights, analizó las políticas de austeridad de España desde una perspectiva de derechos humanos. Los datos de ingresos mostraron que un cuarto de la población y casi un tercio de todos los niños estaban en riesgo de pobreza y exclusión social. También había enormes diferencias regionales.

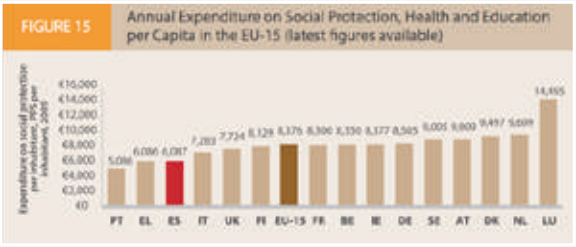
España aprobó el mayor recorte presupuestario de su historia democrática en mayo de 2012, un total de €27,3 mil millones. El motivo era reducir el déficit público. Sin embargo, expertos advirtieron de que estos recortes se hicieron a costa de la accesibilidad y sostenibilidad de los servicios sociales básicos.

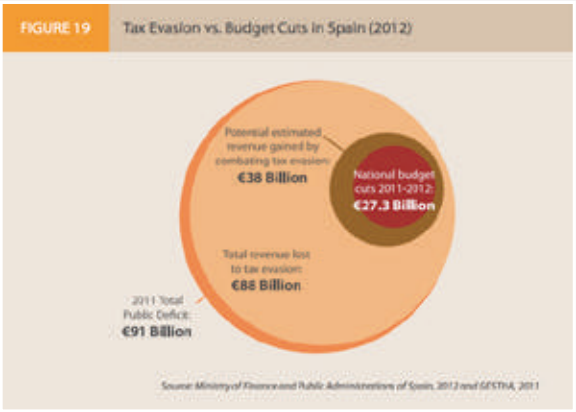
De acuerdo a una generalizada percepción errónea, la crisis financiera en España se creía que estaba causada por el gasto excesivo. De hecho, España estaba entre los países con menor gasto en Europa en protección social, salud y educación.

España tenía una gran economía informal, que causó una pérdida significativa de recaudación tributaria. El sindicato de supervisores fiscales calculó que si España pusiera el tamaño de su economía informal en línea con los estándares de la Unión Europea, sería capaz de generar €38 mil millones, excediendo el total de recortes presupuestarios para 2012.

Los investigadores concluyeron que centrándose casi exclusivamente en los recortes de gasto público, las personas estaban siendo privadas de sus derechos sociales fundamentales. Al no considerar alternativas para reducir el déficit, España no cumple con sus obligaciones bajo el Pacto Internacional de Derechos Económicos, Sociales y Culturales.







HOY ESTÁ, MAÑANA QUIZÁS NO: PRESERVANDO VÍDEOS Y FOTOS EN LÍNEA

Imagine que has encontrado y verificado un vídeo en línea que claramente evidencia una violación de derechos. El vídeo tiene el potencial de reforzar un caso o campaña de defensa en la que estas trabajando, así que guardas el enlace.

Unos pocos días más tarde, el vídeo ya no está...

Los vídeos y fotos en línea pueden desaparecer con rapidez, especialmente si son muy gráficos o tratan de asuntos sensibles para los derechos humanos. Desde enero a junio de 2015, YouTube retiró más de 5.700 vídeos debido tan solo a peticiones de gobiernos. Este es el motivo porque nunca debe tratar las plataformas en línea como unidades de almacenamiento de datos. Los vídeos pueden ser borrados por quien los subió o por la misma plataforma que los recibió por múltiples razones, incluyendo una violación de las condiciones del servicio, quejas de los usuarios, infracciones del copyright, cancelación de cuenta, o si la plataforma cierra por completo.

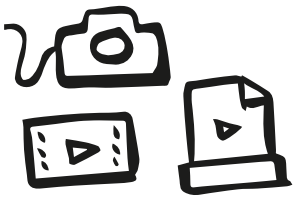
Preservar contenido en línea como fotos y vídeos, incluyendo sus metadatos, asegurará que podrá acceder a ellos en el futuro y ayudará a mantener la integridad de la investigación, le permitirá catalogar los datos y establecerá una cadena de custodia para su uso en ámbito legal

Cómo descargarlos

Al buscar en Google 'download Facebook video' (o 'descargar vídeo Facebook') revela varias herramientas gratuitas, como ***VideoVault***, para preservar las fotos y vídeos en línea, lo que también se conoce como "scraping" (forzar descarga). También hay complementos denavegador y scripts personalizados disponibles para descargar grandes cantidades de contenidos. Tenga en cuenta que hacer scraping del contenido viola las condiciones de uso de muchos sitios web. Es importante ser responsable en cuanto a la manera de guardar, compartir, y acreditar/enlazar al creador original o a quien subió el contenido.

Cuidado: podría haber troyanos maliciosos en el software para scraping, que una vez descargados, pueden causar daños a sus datos y privacidad. Busque software de código abierto que tenga buenas revisiones, y descargue siempre el software directamente desde el sitio del desarrollador o una fuente de confianza.

Sus actividades en línea no son anónimas. Para evitar la vigilancia especifica sobre el trabajo en derechos humanos, considere usar una VPN al buscar y descargar materiales sensibles.



En profundidad

Pasos básicos de preservación

1. **Decide qué contenido es el más relevante** para tu proyecto y qué archivos quieres conservar. Trata de descargar el archivo más grande posible (el de mayor calidad) y guardalos en su formato original.
2. **Usa un modo consistente de organizar sus fotos y vídeos**. Por ejemplo, nombra una carpeta en función del año, mes y día: 2016 03 16. Dentro de la carpeta, nombre los archivos de forma que sean listados en orden cronológico: 00001.AVI, 00002.AVI, etc.
3. **Usa un archivo de texto aparte para documentar los metadatos**. Si la grabación es violento o muy gráfico, incluye una nota clara sobre esto para prevenir al público. El documento de texto debe estar guardado junto al archivo de vídeo o imagen. Si estás recopilando grandes volúmenes de contenidos, considera crear un catálogo.
4. **Guárdalo en una ubicación segura** como la vivienda de un aliado de confianza, o una caja de seguridad en la oficina de una ONG bien establecida, y realiza una copia de seguridad en dos unidades o dispositivos separados que sean conservados en distintas ubicaciones. Considera usar un almacenamiento en la nube especializado explícitamente en almacenamiento seguro de datos, como SpiderOak o TeamDrive.
5. **Compruebe sus archivos y dispositivos periódicamente**.

Para guías detalladas sobre estos pasos, visite *archiveguide.witness.org*

Capturar streams de vídeo en vivo

Los streams en vivo y en directo pueden proporcionar una excelente evidencia inalterada en tanto sean archivados de alguna manera durante la emisión. Muchas plataformas archivan automáticamente los streams en vivo. Si no, tienes que anticiparte a la necesidad y tener software instalado en tu dispositivo para capturarlos.

VPN o "Virtual Private Network"(red privada virtual), es una tecnología que crea una conexión segura sobre una red pública como Internet. Usar 'proxys' VPN puede ayudarle a eludir el filtrado de Internet. Puede conocer más acerca de VPNs y proxys en Security in a Box, una guía del Tactical Technology Collective y Frontline Defenders.

ORGANIZANDO TU CATÁLOGO DE FOTOS Y VÍDEOS

Al trabajar con grandes cantidades de vídeo o fotos, es crítico usar metadatos para la catalogación efectiva. Esto permite a los investigadores identificar rápidamente los archivos correctos, y ahorrar un tiempo valioso.

¿Qué va en la colección?

Antes de elaborar un catálogo, es útil identificar la utilidad esperada, los objetivos y usos deseados del catálogo. Esto te ayudará a asegurar que el contenido que recopilas y catalogas es relevante.

- **¿Por qué existe el catálogo? ¿A qué objetivos sirve?** Ej., defensa de derechos, casos legales, información para medios, concienciación pública, registro histórico de un único incidente o de violaciones de derechos generalizadas, etc.
- **¿Cuál es el ámbito del catálogo?**
  - ¿Qué vídeos o imágenes aceptarás?
  - ¿Qué no aceptarás?
  - ¿Cómo te llegarán esos datos?
  - ¿Qué fuentes o formatos recogerás? Testigos presenciales, noticias / medios, streams de video en vivo, etc.?
- **¿Qué riesgos estás dispuesto a tomar?** ¿Tendrás grabaciones que podrían ponerte a ti y a otros en riesgo, o ser citado judicialmente?
- **¿Precisan sus datos ser compatibles con los sistemas informáticos de alguien más?**

Acceso: Identifique a sus usuarios y contribuidores

Comprender quién usará y contribuirá al catálogo te ayuda a tomar decisiones sobre el accesos y los permisos. Al considerar asuntos de seguridad, identifica a qué amenazas puedes enfrentarte si el catálogo se hace público o se almacena en una plataforma no segura.

- **¿Quiénes son los usuarios?** Determina quién debe tener acceso a su contenido.
- **¿Cómo manejará los derechos de los usuarios?** Ej., la atribución a un individuo u organización según licencia Creative Commons.
- **¿El catálogo será público o privado?** ¿Cuáles son las políticas de acceso?
- **¿Quiénes son los contribuidores?** ¿Qué nivel de conocimientos técnicos tienen? ¿Qué idiomas hablan? ¿Qué formatos de archivo usan?

Establecer una dinámica de trabajo y seleccionar una plataforma

- **¿Cuál es su dinámica de trabajo para asimilar, verificar y catalogar contenido?** Ej., informes de testigos, formulario en línea, hoja de cálculo, formulario impreso, etc.
- **¿Qué plataformas satisfacenlos requisitos de tu estructura de datos?**
- **¿Cuáles son tus restricciones técnicas?** Ej., sin Internet, fondos limitados, sin expertos técnicos, etc.
- **¿Es compatible la plataforma con tu entorno de informático?**
- **¿Qué idiomas necesitas que soporte?**
- **¿Cuáles son los riesgos de seguridad inherentes de la plataforma?** ¿Son compatibles con sus requisitos de seguridad?
- **¿Qué plataformas ofrecen la mejor seguridad para tus datos?** Piensa en la seguridad mientras los datos se transmiten, 'información en movimiento', y mientras están almacenados, 'información en reposo'.
- **¿Cómo compartirás la información con tu usuario final?**

En profundidad

Ejemplos de archivos en línea

El ***Chechen Archive*** comenzó a recopilar fotos, vídeos, y audios de la guerra de Chechenia que se desencadenó en 1994. Para hacer más fácil encontrar, usar y visualizar la información de los archivos, crearon un catálogo extensivo para capturar los metadatos de cada archivo.

El ***People's Archive of Police Violence*** es un archivo en línea de historias, memorias y relatos de violencia policial tal como fue experimentada u observada por los ciudadanos de Cleveland, Ohio. Vea sus ***Condiciones de Servicio del Contribuidor*** para más detalles sobre qué contenido aceptan.

El ***Syrian Archive*** es un archivo en línea que preserva vídeos que documentan violaciones de derechos humanos y crímenes de guerra cometidos por todos los bandos durante el conflicto sirio en curso. Además de elaborar la base de datos en línea, apoyan a defensores de los derechos humanos en sus esfuerzos de documentación

Estructurando tu catálogo

La colaboración con los usuarios finales ayudará a identificar la mejor estructura para tu catálogo. Por ejemplo, los abogados especialistas en derechos humanos pueden decirle que necesita los siguientes metadatos: fecha y localización de un crimen registrado, tipo de crimen, número de identificación del agente, e información de contacto del videógrafo. Por otro lado, un defensor de derechos puede que necesite conocer el nombre de una víctima, o dónde fue publicado el vídeo por primera vez.

- **¿Qué información necesita cada tipo de usuario final para utilizar la colección?** Considera involucrar a usuarios finales en el proceso de desarrollo.
- **¿Cuál es el conjunto de metadatos mínimo?** ¿Qué elementos se requieren, cuáles están recomendados, cuáles son opcionales?
- **¿Cuánto tiempo debe pasar catalogando?**
- **¿Necesitas preservar y catalogar la cadena de custodia porque su documentación podría ser usada para acusaciones criminales en el futuro?**
- **¿Qué información necesitas que sea retenida por motivos de seguridad?**

Retención: Planificando una expectativa de vida realista para tu catálogo

Conocer el periodo esperado de uso para tu catálogo te permiterá planificar mejor tu proyecto, asignar recursos y definir el éxito del proyecto.

- **¿Durante cuánto mantendrás el catálogo?** ¿Conservarás ciertos tipos de contenido más tiempo que otros?
- **¿Qué ocurrirá luego con el catálogo?** Decide sobre un plan de sucesión: eliminación responsable, entrega de los datos a terceros, etc.
- **¿Es realista tu política de retención?** Ej., ¿puedes permitirte seguir con lo que estás planificando durante todo el tiempo que estás planeando hacerlo? ¿Tendrás personal dedicado para mantener, actualizar y controlar el contenido, para toda la vida de la colección?

Ejemplos de plataformas

- Google Sheets/Google Forms
- Excel Spreadsheet
- *Filemaker Pro*
- *Martus*
- *Omeka*
- *Corroborator*

Caso de estudio

Usar vídeo para exponer patrones de abuso en desalojos forzados en Brasil

En 2012, ***WITNESS*** colaboró con activistas, abogados e investigadores, para amplificar y documentar casos de desalojos forzados en Río de Janeiro, y contrarrestar las afirmaciones del gobierno acerca de que no hubo violaciones de derechos antes, durante, o después de los desalojos forzados relacionados con la construcciones para el Mundial de Fútbol de 2014 y los Juegos Olímpicos de 2016. Usaron Google Forms para recopilar, catalogar, contextualizar, y sistematizar más de 100 vídeos de YouTube, fuentes de testigos presenciales, e informaciones de activistas y medios. Los datos se usaron para crear un informe sobre el impacto de los extensos desalojos.

La gráfica del lateral muestra los distintos tipos de violaciones de derechos que ocurrieron durante los desalojos.

WITNESS Media Lab ofrece ejemplos e ideas sobre cómo visualizar tu catálogo.

Foto: "***Luchando por la justicia en Brasil***" Protesta anti-deshaucio en Maua, Brasil 2013, por CAFOD Photo Library en Flickr, CC-BY-NC-ND 2.0 ***https://www.youtube.com/watch?v=2eAIKhFj0m4***

COMO SE VE DESDE EL CIELO: SATÉLITES Y DRONES

Como las plataformas de información aérea y de satélite son cada vez más usadas en sectores que van desde el forestal y agrícola al de la planificación urbana y la ayuda humanitaria, la información recopilada se está haciendo cada vez más disponible para usarla también con propósitos de investigación en derechos humanos.

Fotos aéreas y drones

Aunque drones y UAVs (vehículos aéreos no tripulados) pueden parecer futuristas, son un medio sencillo de capturar panorámicas desde el aire, y ya son dispositivos populares tanto para quienes los usan por hobby como para profesionales.

Las vistas aéreas ofrecen una cobertura extensiva del terreno que es útil para investigar y documentar infraestructuras, cambios ambientales, daños por conflictos o desastres naturales, y mucho más.

Si quieres lanzar tu propio dron hay recursos útiles disponibles ***iniciarse, desplegar***, y comprender las ***regulaciones*** nacionales y locales (asegúrate de conocer las reglas o podrías arriesgarte a ser multado, que tu equipamiento sea confiscado, ¡o incluso ser arrestado!).

Foto: AJ+ (Al Jazeera Plus) comparte un

vídeo capturado por un dron volando sobre Alepo, Siria, en 2015, para mostrar claramente los daños a la ciudad tras cuatro años de guerra.

Con más frecuencia los investigadores en derechos humanos usaremos grabaciones de drones encontradas en plataformas en línea como ***Open Aerial Map*** o ***UAViators***. Este tipo de grabaciones, subidas por individuos u organizaciones, bien anónimos o determinados, requieren los mismos pasos de verificación que todos los demás contenidos en línea.

Satélites para derechos humanos

En enero de 2015, The New York Times hizo un reportaje sobre un ataque de ***Boko Haram*** en dos ciudades al noreste de Nigeria. Para mostrar la escala masiva de la destrucción de hogares, usaron imágenes satelitales proporcionadas por Amnistía Internacional y Human Rights Watch. Fue un poderoso ejemplo de cómo las imágenes de satélite puede promover la investigación y la defensa de los derechos humanos.

Las imágenes satelitales ya no son dominio exclusivo de los gobiernos, nuevas tendencias en oferta de imágenes harán este tipo de datos aún más accesibles en el futuro. Pequeños y grandes grupos ya pueden usar imágenes satelitales en su labor diaria en derechos humanos.

Beneficios de las imágenes satelitales

- **Acceso físico**
  Los satélites permiten eludir las restricciones de acceso. En conflictos armados, pueden ser movilizados en lugar de un investigador.
- **Registro histórico**
  Las imágenes satelitales a menudo permiten a los investigadores ir atrás en el tiempo para estudiar cambios en el terreno buscando en plataformas públicas como Google Earth.
- **Visuales**
  Las imágenes satelitales pueden suministrar potentes y conmovedoras imágenes para su uso en trabajos en defensa de los derechos humanos y en campañas de concienciación.
- **Fiabilidad de la fuente y acceso a los metadatos**
  En comparación con las redes sociales, la fuente original de una imagen satelital habitualmente está clara. A menudo viene también con metadatos detallados, como coordenadas o fecha y hora, convirtiéndola en una fuente fiable de datos.
- **Análisis avanzados**
  Los sensores en los satélites captan más información de la que ve el ojo humano, como luz infrarroja o ultravioleta, que se puede usar para resaltar y medir la salud de la vegetación. Estas técnicas sirven, por ejemplo, para medir y visualizar el impacto de derrames de crudo, documentar rastros de movimientos militares durante conflictos armados, o medir ataques contra el medio ambiente como indicadores de genocidio.

Limitaciones de las imágenes satelitales

- **Interpretación**
  El análisis de imágenes puede ser susceptible a la interpretación errónea, especialmente si es realizada por analistas o investigadores no instruidos en análisis de imágenes satelitales. Por ejemplo, se puede interpretar la tierra removida como un enterramiento masivo o un huerto. La corroboración y verificación cruzada con otra información es, por tanto, crucial.
- **Disponibilidad**
  Los satélites comerciales o de gobiernos no recorren persistentemente cada lugar del planeta y puede haber vacíos manifiestos en la disponibilidad de ubicaciones de las imágenes, especialmente en zonas muy remotas o políticamente sensibles.
- **Nubes**
  Incluso si hay imágenes disponibles en la fecha deseada, la presencia de nubes puede entorpecer fuertemente la usabilidad de las imágenes.
- **Áreas problemáticas**
  Las imágenes satelitales son beneficiosas para una amplia variedad de asuntos de derechos humanos, pero pueden ser de uso muy limitado para otras áreas de interés. Las desapariciones forzadas, por ejemplo, son difíciles o imposibles de documentar mediante imágenes satelitales.

Caso de estudio

Exponer una masacre y demoliciones en Nigeria con imágenes de satélite

Siguiendo informes acerca de demoliciones y matanzas en Zaria, Nigeria, en diciembre de 2015, analistas de Amnistía Internacional revisaron imágenes de satélite gratuitas en línea de Google Earth para encontrar soporte de evidencias de ***matanzas a gran-escala ilegales por parte de los militares nigerianos***, exponiendo un burdo intento de las autoridades de ocultar pruebas. Afortunadamente, en este caso Google Earth contenía imágenes actualizadas a las que se podía acceder con la opción "Imágenes históricas" ubicado en la parte superior izquierda. Esta característica le permite ver cómo cambian los paisajes con el tiempo. En el caso de Zaria, ayudó a identificar varias áreas demolidas, incluyendo un cementerio y una mezquita, además de la aparición de un probable enterramiento masivo. La función "Guardar mapa" se usó para descargar mapas para informes. Todas las imágenes de Google Earth se pueden usar libremente para ***propósitos no comerciales***. Pagar por la ***versión pro*** habilita descargas de imágenes de alta resolución que son mejores para la impresión.

Para ayudar al impacto visual de las imágenes satelitales en informes en línea, es posible crear un control deslizante que permite cambiar entre imágenes yuxtapuestas de manera sencilla, lo que permite al lector explorar cambios temporales por si mismo. Una herramienta fácil y gratuita para incrustar estos deslizadores es ***Juxtapose***.

Ejemplo 1: Demolición de una mezquita
Antes: *https://c2.staticflickr.com/8/7754/26656228073_56a3c2f374_c.jpg*
Después: *https://c2.staticflickr.com/8/7236/27261977225_9774490f7e_c.jpg*

Ejemplo 2: Enterramiento masivo
Antes: *https://c2.staticflickr.com/2/1507/25903760253_1713948455_c.jpg*
Después: *https://c2.staticflickr.com/2/1704/25901693544_717cff591d_c.jpg*

Vea las yuxtaposiciones antes-después para todas las localizaciones en el ***Blog de Google Earth***.

Ejemplo 1: Demolición de una mezquita

Ejemplo 2: Enterramiento masivo

Fuentes de imágenes satelitales con resolución inferior al metro

- **Google Earth**: Puede ser una herramienta altamente útil como fuente de imágenes satelitales gratuitas. Sin embargo, a veces tiene baja resolución en algunas zonas como resultado de la presión política.
- **TerraServer**: Un proveedor de imágenes satelitales de DigitalGlobe. Se puede usar de forma gratuita en apoyo de la investigación básica, y a menudo proporciona imágenes más actualizadas que Google. Tendrá que pagar una pequeña tarifa por descargar las imágenes recientes. Adicionalmente, tiene que pagar por una licencia si desea usar la imagen públicamente.
- **Proveedores comerciales de imágenes**: Los principales proveedores de imágenes de satélite de muy alta resolución son ***DigitalGlobe***, ***Airbus***, y ***Urthecast*** (***Deimos-2***). La resolución para estos satélites varía entre 0.3-0.75 metros (aproximadamente el tamaño del sujeto u objeto más pequeño que se puede identificar en una imagen). El tamaño mínimo a encargar para la compra de imágenes es de 25 Km2. Los precios para este tamaño parten desde aproximadamente $175.
  - **Microsatélites**: Un gran avance de compañías como ***Planet Labs*** o ***TerraBella*** es que en un momento dado proveerán una constelación completa de satélites, esto es, están creando un sistema de monitoreo constante desde el espacio. Las compañías antes mencionadas sólo pueden proporcionar capturas de ciertas áreas del planeta. Algo a tener en cuenta es el ***vídeo satélite***, que tendrá grandes implicaciones para la investigación en derechos humanos. Una desventaja de estos microsatélites es que la mayoría de ellos actualmente tienen una resolución más baja que otras alternativas, es decir, son visibles menos detalles en la imagen.

Consideraciones de datos responsables

RIESGOS DE SEGURIDAD DE LA VIDA REAL

La protección física y la seguridad en un contexto de datos digitales requieren un enfoque y aproximación diferentes. Para la recopilación tradicional de documentación, los profesionales en derechos humanos a menudo siguen las mejores prácticas que les marca su intuición para protegerse a si mismos y los individuos que entrevistan: reunirse en lugares seguros, ocultar información identificadora confidencial, y evitar tomar caminos que pueden llevar al peligro.

Para muchos, la seguridad física para nuevos métodos de datos no es tan intuitiva aún porque a menudo entre el investigador y los individuos aludidos en los datos no hay relación personal.

La seguridad física y de datos digitales están vinculadas estrechamente. El propósito de la seguridad digital no es sólo proteger los datos sino también proteger a los individuos que contribuyeron a ellos, o que fueron representados en ellos.

Si un hacker compromete un servidor, o un control oficial confisca un disco duro, los nombres, caras, y/o la información de un gran número de víctimas u otros individuos vulnerables estará comprometida. Es tu obligación tomar todas las medidas para protegerte a ti mismo y a los demás involucrados de daños adicionales.

Las personas involucradas en los datos entran en tres categorías, a veces solapadas: aquellos que los capturan, aquellos que los comparten en línea o en un disco duro externo, y aquellos cuya información está contenida en los datos.

A menudo las personas no se dan cuenta de que un vídeo que están publicando en línea contiene información sensible. Si tu, como profesional en derechos humanos, decides usar un vídeo para una campaña, la fuente y el creador pueden convertirse en objetivo de ataques por estar afiliados con tu grupo, incluso si nunca supieron sobre ustedes.

Aquellos retratados en los materiales digitales pueden no haber dado su consentimiento, o incluso no ser conscientes de que estuvieran siendo filmados. Si revelas públicamente sus rostros o sus nombres en el contexto de una violación de derechos humanos, sin darte cuenta, puedes causar que sean hostigados o que se abuse de ellos aún más.

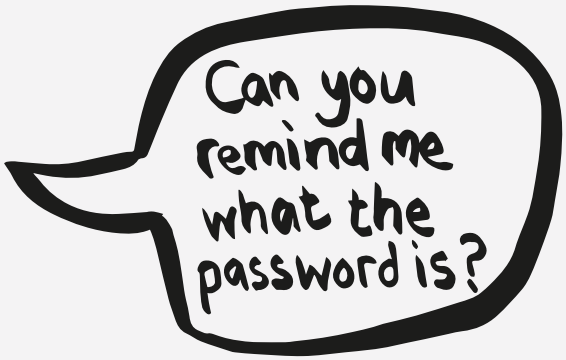
En el caso de que hagas públicos los datos, o que haya una brecha de seguridad en tu organización, la fuente y los individuos retratados se exponen a un mayor riesgo de daño físico, incluso si su información ya se encontraba publicada en línea. Peor aún, puede ser difícil informar a cualquiera de estos individuos del súbito aumento en su riesgo, ya que es improbable que el investigador tenga información de contacto u otros medios de llegar a aquellos identificados. Por tanto, es crítico evitar la publicación de los datos en primer término.

Caso de estudio

Ingeniería social: ¿Con quién está hablando realmente en línea?

El activismo en derechos humanos en Irán proporciona un ejemplo contundente de la conexión entre seguridad digital y física. Recientemente, las autoridades iraníes ***han usado ingeniería social*** perseguir defensores de los derechos humanos a través de comunicaciones vía correo electrónico, Facebook, y LinkedIn. La ingeniería social es el acto de usar circunstancias personales y manipulación psicológica para convencer a un individuo de que es seguro romper los protocolos de seguridad y divulgar información privada. ***Un agente del gobierno podría crear un perfil en un medio social*** usando el nombre de un conocido activista, e iniciar conversaciones que induzcan a otros activistas a revelar información sensible.

La República Islámica ha usado esta táctica con bastante éxito, conduciéndoles a la detención e interrogatorio de prominentes defensores de los derechos humanos. Incluso ***funcionarios del Gobierno de EEUU han sido víctimas*** de la ingeniería social, divulgando información de modo no intencionado al Gobierno de Irán. La ingeniería social a menudo es más efectiva que el tradicional hackeo porque no se basa en ninguna destreza técnica, y ataca las vulnerabilidades de los individuos en lugar de las de los sistemas digitales.



"¿Me puedes recordar cual es la clave?"

Para evitar ser atacado mediante técnicas de ingeniería social, sea cauteloso en todas sus comunicaciones. Formule preguntas clarificadoras o personales para asegurarse de que la persona con la que está hablando es quien dice ser, e interrumpa la comunicación si tiene alguna duda de la identidad de quien esta detrás de un cuenta en un servicio digital. Evite también compartir información sensible a través de redes sociales o correo electrónico, sin tener implementadas medidas de seguridad adicionales.

DATOS RESPONSABLES

Datos responsables consisten en:
El deber de asegurar el derecho de las personas al consentimiento, privacidad, seguridad y propiedad en torno a los procesos de información que recopilan, analizan, almacenan, presentan y reutilizan los datos, a la vez que se respetan los valores de transparencia y apertura.
Responsible Data Forum, definición de trabajo, septiembre de 2014

Para permanecer al día de cuestiones en torno a los datos responsables, vea ***https://responsibledata.io*** y suscríbase a la lista de correo en ***https://engn.it/rdmailinglist***

Ser juicioso y proactivo en lo referente a cómo trabajar con datos digitales es esencial para asegurar la seguridad y bienestar de la gente con la que trabajas. El abanico de cuestiones éticas que podrían surgir, se podrían denominarse como **desafíos de datos responsables**. No hay una política establecida que vaya a funcionar para todas las situaciones, pero te invitamos a que reflexiones sobre los siguientes asuntos dentro de tu contexto:

- **Consentimiento informado**
  Especialmente dentro del ámbito de las violaciones de derechos humanos, obtener consentimiento informado puede suponer mucho más de lo que puedas pensar en un principio. Asegúrate de que la gente de la que está obteniendo consentimiento lo está proporcionando voluntariamente, que comprenden completamente aquello a lo que están consintiendo, y que están en posición de tomar este tipo de decisiones.
- **Minimización de datos**
  En interés de la privacidad y la reducción del riesgo, intenta recopilar la cantidad mínima de datos necesarios para tu propósito específico.
- **Datos personales**
  Siempre que sea posible, si tienes nombres, fechas de nacimiento u otra información con capacidad de identificación personal, trata de desvincularla o borra lo que no necesites.
- **Datos sensibles**
  Sea consciente de dónde se almacenan los datos sensibles sobre raza, etnicidad u orientación sexual, si están en tus servidores o en un país extranjero (ej., al usar un servicio de Google) por si acaso pudieran dejar expuestos a los individuos a algún riesgo.
- **Parcialidad implícita**
  Los datos reunidos de otras fuentes pueden ocultar sesgos. Piensa detenidamente acerca de las decisiones humanas que se tomaron durante el análisis.

Información proveniente de redes sociales

Muchas organizaciones parecen pensar que la información 'de dominio público' se puede usar libremente para cualquier propósito. Sin embargo, incluso si una persona accede a que su información 'se haga pública' de cierta manera, no significa que la información sea éticamente adecuada para cualquier uso.

Cuando una persona publica acerca de una violación de los derechos humanos en Twitter, no significa que automáticamente consienta en convertirse en el foco de atención de una campaña pro derechos humanos con alcance global. Tienes que contactar con las personas directamente y ayudarles a comprender las posibles consecuencias (positivas y negativas) de atraer más atención sobre si mismos, para que puedan tomar una decisión informada.

Protegiendo la identidad de las personas en redes sociales

Los mensajes en las redes sociales que documentan violaciones de derechos, pueden contener vídeo y/o imágenes de personas que no tenían ni idea de que estaban siendo filmadas. Tanto si eres tú quien personalmente publica estos datos, como si lo haces en nombre de una organización que desea volver a publicarlos, debes proteger a los individuos tanto como sea posible.

Hay varias herramientas útiles para difuminar caras en vídeos y fotografías. Por ejemplo, ***ObscuraCam*** es una aplicación para teléfonos Android que pixela o edita caras. Funciona tanto mientras estáss grabando, como cuando carga algo desde tu biblioteca. Recientemente YouTube también ha añadido una ***característica de difuminado*** que te permite oscurecer caras cuando cargas un vídeo.

¿SON SEGURAS TUS HERRAMIENTAS DIGITALES?

Cuando se trata de hacer copias de seguridad, almacenamiento de archivos, y destrucción de datos, segura, recomendamos consultar Security in a Box de Front Line Defenders y el Tactical Technology Collective.

La seguridad digital no se limita al uso de herramientas y software seguros, sino que se integra en los hábitos y prácticas generales de una organización.

Cuando hablamos de seguridad digital, estamos hablando acerca de dar pasos para proteger los datos, tanto mientras están en tránsito (correo electrónico, chats y SMS), como mientras están almacenados (un archivo guardado en tu disco duro).

Damos estos pasos porque en la recopilación, conservación y difusión de datos sensibles, especialmente datos relativos a derechos humanos, hay implicaciones en cuanto a ética y seguridad.

Tenemos una responsabilidad de proteger la privacidad de aquellos cuyos nombres e identidades están representados en nuestros datos, y que confían en nosotros con su información.

Nuevas herramientas y servicios hacen distintas proclamas acerca de la seguridad de sus productos. ¿Cómo sabemos que eso es cierto? Hay algunas preguntas que debemos plantearnos al considerar nuevo software. No es probable que pueda responderlas todas, pero hágalo lo mejor que pueda.

Antes de adoptar nuevo software, pregúntate a tí mismo...

1. **¿Qué significa "seguro" en realidad?**
Decir que un software es "seguro" puede significar distintas cosas. Lee la letra pequeña de cualquier descripción de software. Muchas herramientas que afirman ser "seguras", incluyendo Dropbox, Google y Skype, cifran sus datos mientras viajan entre tu computadora y sus servidores —pero los datos no están protegidos de que las propias compañías accedan a ellos. Algunas herramientas y servicios usan cifrado de maneras que protegen los datos incluso de los propios proveedores de servicio. Es importante comprender esta distinción, y considerar si es relevante para tu proyecto mantener ocultos los datos de los proveedores de servicios.

2. **¿Ha sido auditado el software de forma independiente?**
No te limites a confiar en los desarrolladores de software cuando prometen ofrecer seguridad, especialmente cuando el software es completamente nuevo. Incluso con las mejores intenciones, implementar cifrado de forma correcta es difícil. Sólo usa software que haya sido auditado por alguien en quien confíes. Preferiblemente el software debe ser de "código abierto", y este estar disponible para su escrutinio público. E incluso entonces, no puedes estar seguro de que tras un resultado de auditoría impecable no se escapado algunas vulnerabilidades. Mantén siempre un saludable escepticismo.

3. **¿Quién tiene en su poder los datos - y por cuánto tiempo?**
Cuando uses un servicio en línea para comunicarse, crear o archivar información, debes preguntarse quién "tiene en su poder" los datos, especialmente si se almacenan en los servidores de un proveedor de servicios como Facebook, Twitter o Dropbox. Las respuestas es probable que estén sepultadas en las Condiciones de Servicio de las compañías. Cualquiera que sea el servicio que uses para archivar o compartir datos sensibles, debes investigar sus políticas sobre compartición de datos con otras compañías y gobiernos, y qué es lo que puedes esperar que ocurra con los datos si borras tu cuenta, la compañía cambia de propietarios o cierra.

4. **¿Ofrece protección el software contra las amenazas concretas que debes afrontar?**
Comprender tus propias amenazas es importante para valorar si una aplicación o servicio será adecuado para protegerte. En lugar de adoptar una herramienta porque has oído que deberías hacerlo, pruebes a elaborar un "modelo de amenaza" para determinar quién puede intentar acceder a tus datos, y cómo (vea el capítulo ***Una Introducción al Modelo de Amenaza***) de la guía Surveillance Self Defense). Las respuestas a estas preguntas te ayudarán a establecer qué herramientas son las más apropiadas. Para conocer más acerca de cómo llevar a cabo un análisis de contexto, mira la sección Explore del ***Holistic Security Manual*** (manual de seguridad holística).

5. **¿Te dejará expuesto el uso del software o servicio?**
En algunos lugares el uso de cifrado es ilegal. En otros no lo es, pero igualmente levanta sospechas de las fuerzas de la ley o de agencias de inteligencia. Esto puede llevarles a vigilar la actividad de una persona simplemente porque ha comenzado a usar software de cifrado. Es importante comprender cual es tu riesgo; en algunos contextos, no usar cifrado puede ser más seguro, incluso aunque los datos se almacenen y envíen no protegidos (¡algo que también es arriesgado!). Puede permitirte mantener un perfil bajo y atraer menos atención. Conocer tu contexto es esencial para hacer este tipo de valoración.

6. **¿Es práctico para tí adoptar este software o servicio?**
Algunos servicios o software pueden encajar bien en los procesos que actualmente estás usando para recopilar, almacenar, analizar, y compartir datos. Otros pueden requierir una reconversión importante a nuevas dinámicas de trabajo. Incluso para el software que promete seguridad, su uso práctico es una cuestión importante a indagar. Si es demasiado difícil de usar o no es probable que su uso sea una práctica sostenible, intentar adoptarlo puede acabar siendo una pérdida de valiosos recursos en tiempo, dinero y energía.

7. **¿Estás adoptando esta aplicación por las razones correctas?**
Hay muchas razones por las que podríamos estar interesados en un nuevo servicio o herramienta: Puede estar atractivamente diseñado, tener un nombre interesante, prometer un servicio novedoso, estar creciendo en popularidad, etc. Realiza un análisis frío y crítico de las razones por las que estás considerando adoptar una herramienta y asegúrate de que parecen ser las razones correctas, dadas tus necesidades y obligaciones éticas y de seguridad.

Es muy poco probable que algún software o servicio cubra todas estas necesidades. La meta no es encontrar un unicornio que satisfaga todo requerimiento, sino tomar decisiones informadas e intencionadas acerca del software que adoptamos. Tras leer estos consejos, ¿te sientes de forma distinta sobre esa herramienta o servicio que has adoptado recientemente? ¿Sigue siendo la elección correcta para tí?

En profundidad

Transparencia respecto de los riesgos.

Algunos desarrolladores publican "modelos de amenaza" y vulnerabilidades conocidas en su sitio web en aras de la transparencia. Como buenos ejemplos, revisa la documentación de ***Scramble.io*** (software de correo electrónico seguro) y ***Cryptocat*** (software de chat seguro). Cada vez más compañías publican también informes de transparencia que destacan cosas como peticiones oficiales de información de usuarios y notificaciones legales de remoción de contenido. Por ejemplo, vea el ***Twitter's Transparency Report*** (Informe de Transparencia de Twitter). Estos informes son voluntarios y difíciles de verificar, pero aún así pueden ofrecer contextualización en torno a la seguridad de los servicios.

Ejemplo

¿Debe Jon usar WhatsApp para trabajo en derechos humanos?

Jon es un activista pro derechos humanos en Kampala, Uganda, y está recopilando informes de violencia contra personas LGBTI. La homosexualidad es ilegal en Uganda, y el grupo de Jon es monitoreado de forma rutinaria por la policía. Jon acaba de comprar su primer smartphone, y está considerando usar la aplicación de chat WhatsApp. Muchos de sus amigos la usan, y ha oído que es segura.

Esto es lo que decidió Jon...

WhatsApp implementó el cifrado que utiliza la aplicación Signal en 2016, que es de código abierto, verificable y de buena reputación. Pero el propio WhatsApp no es de código abierto y no hay auditorías públicas del código, así que Jon no puede estar completamente seguro de su seguridad. Además, los mensajes de WhatsApp están cifrados en tránsito, pero no cuando se encuentran cifrados en el dispositivo, así que un teléfono robado podría ser vulnerable. Jon no es un experto usando WhatsApp, pero pregunta a un colega y decide investigar otras aplicaciones de mensajería, incluyendo ***OpenEvsys*** y ***Martus*** que están desarrolladas para propósitos de derechos humanos.

TRAUMA SECUNDARIO Y TEPT

Los profesionales en derechos humanos están comprometidos en ayudar a otros. Como tales, el bienestar y la seguridad a menudo son considerados lujos u objetivos egoístas, particularmente al operar en zonas de conflicto. Es esencial que tanto organizaciones como individuos trabajen para contrarrestar esta creencia equivocada. El reconocimiento de la importancia de la seguridad y el bienestar fomenta la adaptabilidad y la agilidad, mejora la gestión y la movilidad de los recursos, y habilita la preparación para los riesgos inherentes al trabajo en derechos humanos.

La seguridad esta relacionada a la protección y bienestar físico, la salud, las finanzas, la discriminación, la privacidad, etc. Las amenazas a la seguridad varían de persona a persona y de grupo a grupo. Para algunos, su religión o su orientación sexual pueden suponer el mayor de los riesgos de seguridad. Comprender estos asuntos desde la perspectiva de todos los que estén involucrado en tu trabajo, es el primer paso en el fomento de un entorno productivo y seguro.

Llevar a cabo y mantener los siguientes análisis te ayudará a crear estrategias, planes y acuerdos compartidos para promover la seguridad y el bienestar:

- Explora las tendencias políticas, económicas, sociales, tecnológicas, legales y ambientales inherentes a tu trabajo.
- Identifica y analiza amenazas de seguridad concretas y toma las medidas necesarias para prevenirlas o responder a ellas.
- Identifica a tus aliados y oponentes, sus intereses y su potencial para asistirte o para actuar en tu contra.
- Identifica y separa en categorías la información y datos privados, y toma medidas para protegerlos de pérdida o daño.

Atenuar el trauma secundario producido por sus datos

El volumen sin precedentes de contenidos audiovisuales disponibles para los investigadores en derechos humanos de hoy día tiene considerables beneficios, pero también considerables riesgos. Una investigación de ***Eyewitness Media Hub*** muestra que el 82% de los investigadores en derechos humanos ven imágenes perturbadoras sentados en sus escritorios, varias veces al mes.

La exposición a demasiado trauma primario puede conducir a un trauma secundario, que a su vez puede llevar a un trastorno de estrés post-traumático (TEPT). Organizaciones, administradores, e investigadores, deben reconocer y paliar estos riesgos. Eyewitness Media Hub lista varios desencadenantes que pueden ser perturbadores para los individuos, muchos de los cuales son comunes en las fuentes de datos digitales, incluyendo:

- **Sorpresa**: El individuo no espera visionar un vídeo violento.
- **Exposición repetida**: El individuo tiene que ver un vídeo violento repetidamente.
- **Asociación personal**: El contenido recuerda al investigador una situación o una conexión personal con el hecho.
- **Audio de sufrimiento humano**: Oír el sonido asociado a un acto de violencia hizo más perturbador al vídeo.
- **Sentimientos de culpa**: Los investigadores en derechos humanos informan de un habitual sentimiento de culpa al traumatizarse por la violencia que se está infligiendo sobre alguna otra persona.

Signos de trauma secundario

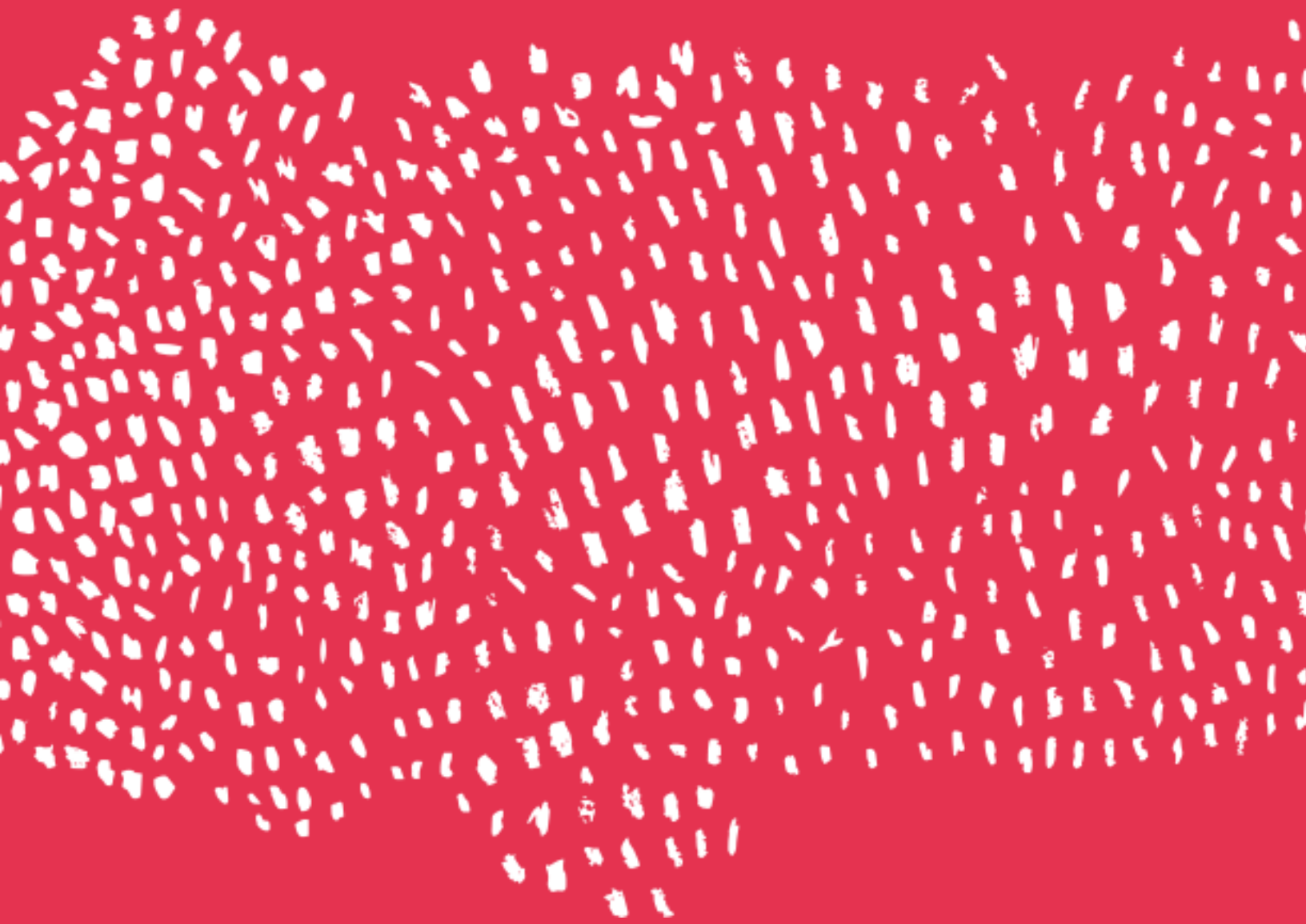
- Dificultad para manejar sus emociones.
- Dificultad para aceptarse o sentirse bien contigo mismo.
- Dificultad para tomar buenas decisiones.
- Problemas para fijar límites. Ej. tomar demasiada responsabilidad, tener dificultades para abandonar el trabajo al final de día, tratar de inmiscuirse y controlar las vidas de los demás.
- Problemas con tus relaciones.
- Problemas físicos como dolores y achaques, indisposición, o accidentes.
- Dificultad para sentirte conectado con lo que ocurre alrededor y contigo mismo.
- Pérdida de significación y esperanza.
- Incremento del abuso de sustancias, alcohol en particular.
- Comilonas desmedidas.
- Aislarse uno mismo de amigos y colegas.

Los individuos que sufren trauma secundario pueden experimentar ninguno, alguno, o todos estos síntomas. Cualquier cambio de comportamiento repentino debe ser investigado.

Pasos inmediatos para evitar el trauma secundario

1. Controla la frecuencia con la que el personal se expone a contenido traumático.
2. Elimina la exposición repetida innecesaria.
3. Revisa los procedimientos de ordenamiento y etiquetado para reducir la exposición innecesaria al material explícito.
4. Prueba distintas formas de ver el contenido. Algunos encuentran que concentrarse en ciertos detalles, por ejemplo vestimenta, y evitar otros, como rostros, puede ayudar a crear una distancia emocional.
5. Ajusta el entorno en que se ve el material: reduce el tamaño de la imagen o vídeo, o ajusta el brillo/resolución de la pantalla.
6. Apague el sonido cuando sea posible.
7. Tómate descansos frecuentes de la pantalla. Mira algo agradable, estira las piernas o da un paseo.
8. Cuando envíes correos con contenido gráfico, añade una advertencia del contenido en la línea del asunto.
9. Etiqueta claramente todos los elementos al archivarlos, para que nadie se exponga accidentalmente al contenido explícito.
10. Elabora tu propio plan de cuidado propio. Nuestras investigaciones muestran que los individuos altamente adaptativos es más probable que hagan ejercicio con regularidad, mantengan intereses y hobbies externos, e inviertan tiempo en sus conexiones sociales cuando se enfrentan al desafío del estrés relacionado con un trauma.
11. Establece redes de apoyo entre compañeros dentro de las organizaciones, para hablar sobre el horrible contenido que han tenido que encontrarse.

El TEPT que surge del trauma secundario puede tratarse profesionalmente. Si crees que tú o un colega pueden estar sufriendo de TEPT, busca ayuda profesional de inmediato.



A dónde ir desde aquí

CÓMO ENCUADRAR TU INVESTIGACIÓN

Antes de entrar en análisis, piensa con detenimiento sobre lo que representan tus datos y qué conclusiones válidas puedes extraer de ellos. Esta sección te ayudará a establecer la representatividad de un conjunto de datos y precisar las incertidumbres para evitar conclusiones inapropiadas o incorrectas.

Establecer qué tipo de muestra son tus datos

Hay tres tipos de muestras. El tipo de muestra que tienes depende de cuántas unidades de análisis tiene y de cómo fueron seleccionadas.

- **Muestra completa**: una población entera. Otros términos para muestra completa son "censo" o "lista completa".
- **Muestra probabilística**: las unidades de la población fueron seleccionadas mediante un mecanismo probabilístico. Este mecanismo asegura que la probabilidad de elección para cada unidad de población es conocida.
- **Muestra de conveniencia**: las unidades fueron seleccionadas por un mecanismo no probabilístico. Para cada unidad de la población no se conoce la probabilidad de ser seleccionada en la muestra, aunque es muy alta para algunas unidades, y muy baja o cero para otras. En la investigación en derechos humanos, las muestras de conveniencia son el tipo más probable de muestras de datos disponibles.

Determinando qué conclusiones puedes extraer

El proceso de evaluar y extraer conclusiones de los datos se llama "inferencia". Hay dos tipos de inferencia:

- **Inferencia estadística**: extrae conclusiones *acerca de la población*, en base a la muestra. Estas conclusiones sólo son válidas si tiene una muestra completa o probabilística.
- **Descripción**: extrae conclusiones sólo *acerca de la muestra* que se tiene.

Haciendo inferencias de muestras completas

Las muestras completas son especiales porque son idénticas a la población, así que los aprendizajes que puedas extraer de la muestra, también serán aplicables sobre la población.

Haciendo inferencias de muestras probabilísticas

Las muestras probabilísticas son representativas de la población si las probabilidades subyacentes de la muestra se corresponden a la población. Como cada unidad en la población tiene una probabilidad conocida de ser seleccionada en la muestra, en promedio, podemos hacer aproximaciones de los valores reales en la población en base a los valores y distribuciones existentes en la muestra (con un rango de probabilidad de error de muestreo). No consideramos a todas las unidades de la población, sino sólo a una muestra representativa de esta, así que llamamos "estimaciones" a estas conclusiones.

En profundidad

Población

En el análisis estadístico, la población se refiere a las unidades de análisis que deseas estudiar.

Ejemplo 1
Deseas saber cuántos refugiados que han ingresado al País X por vía marítima le fue negado el acceso a atención sanitaria. La población sería el conjunto de todos los refugiados que han ingresado al País X por vía marítima y les fue negado el acceso a atención sanitaria.

Ejemplo 2
Estás examinando si es posible que las instalaciones que producen flores han causado polución de las fuentes de agua en una determinada región. En este caso, X es el el conjunto de todas esas instalaciones en esa región.

Haciendo inferencias de muestras probabilísticas

Las muestras probabilísticas son representativas de la población si las probabilidades subyacentes de la muestra se corresponden a la población. Como cada unidad en la población tiene una probabilidad conocida de ser seleccionada en la muestra, en promedio, podemos hacer aproximaciones de los valores reales en la población en base a los valores y distribuciones existentes en la muestra (con un rango de probabilidad de error de muestreo). No consideramos a todas las unidades de la población, sino sólo a una muestra representativa de esta, así que llamamos "estimaciones" a estas conclusiones. .

Hacer inferencias de muestras de conveniencia
Las muestras de conveniencia no son representativas de la población. Están sesgadas de formas desconocidas ya que no sabemos qué unidades de la población se dejaron fuera, o qué unidades era más o menos probable que fueran seleccionadas. No permiten aprender de nuestra población, y no debemos exagerar las conclusiones que podamos extraer de la muestra.

Conclusiones que se pueden extraer de muestras de conveniencia

- El número de personas que puede documentar cuyo derecho a atención sanitaria fue violado.
- Compendiar y describir los individuos afectados y los problemas médicos que sufren.
- Crear gráficas para visualizar las violaciones de derechos que documentó. Asegúrate de identificar claramente estas gráficas como compendios de "violaciones de derechos reportadas" o de "violaciones de derechos documentadas" (vea ***este informe de HRDAG*** para un ejemplo de cómo describir los datos de muestras de conveniencia y cómo anotar las gráficas con tales datos).
- Describir las prácticas del estado que ha identificado como conducentes a la denegación del acceso a la atención sanitaria.
- Hacer constar dónde y en qué momentos ha identificado estas prácticas. Si has documentado estas prácticas en varias instalaciones sanitarias por todo el país X y/o repetidamente a lo largo del tiempo, puedes señalar este rango espacial y/o temporal.
- Señalar que la ausencia de informes adicionales de tales prácticas estatales no significa que esas prácticas no ocurrieran. Puede que simplemente no hayas sido capaz de identificar más de ellas.

Para apoyar esta afirmación podrías listar las instalaciones que has podido visitar en un esfuerzo de reunir evidencias adicionales. Las evidencias perdidas podrían no indicar la falta de violaciones de derechos, sino simplemente ser el resultado de no poder investigar en ese área.

- Concluir que las prácticas estatales son un problema que debe tomarse en serio.

Conclusiones que no puedes extraer

- El número de refugiados a los que se les ha denegado el acceso a atención sanitaria. A causa de que es una muestra de conveniencia, no conoces cuántos refugiados no has sido capaz de documentar.
- Deducir qué prácticas estatales son las más y/o las menos comunes.
- Deducir las tendencias espaciales al poner de relieve si las prácticas estatales son más prevalentes en un área en comparación con otra.
- Deducir tendencias temporales al poner de relieve prácticas estatales ocurridas más frecuentemente durante un periodo de tiempo en comparación con otro, y/o si las prácticas estatales se han incrementado, reducido, o estancado con el tiempo.

Si tratas la información de tu muestra de conveniencia como lo que es —tan solo las evidencias de violaciones de derechos humanos que pudo documentar— tendrás una base más fuerte para justificar tus denuncias sobre derechos humanos en público.

Documentando tu proceso de investigación

- Perfilar con claridad la metodología usada para alcanzar una conclusión, hace tus hallazgos accesibles y transparentes, añadiendo legitimidad a tus denuncias.
- La documentación interna y el llevar un archivo te ahorran tiempo y dinero, a la vez que reducen el riesgo de pérdida de información.
- Documentar prácticas exitosas expande tu conocimiento dentro y fuera de tu comunidad. Esto es especialmente relevante con fuentes de datos digitales donde la base de conocimiento todavía está en desarrollo.
- Anota todas las decisiones que tomes y cartografíe las fuentes de datos que has usado. Describe cómo has obtenido cada fuente de datos y cómo has trabajado con cada una.
- Un resumen paso a paso de tu metodología de investigación debe permitir que otros sigan tus pasos, repitan tus hallazgos, y extraigan conclusiones comparables.

Preguntas sobre la muestra que tu metodología debe tratar de resolver

- **¿Cuál es el foco geográfico de tu estudio?**
- **¿Cuál es el foco temporal de tu estudio?**
- **¿Cómo has medido X?**
  - **a. Fuente de datos principal**
    - i. ¿Dónde y cuándo fue descargada?
    - ii. ¿Quién fue el creador/proveedor original? ¿Es creíble esta fuente? ¿Cómo has verificado estos datos?
    - iii. ¿Está disponible públicamente?
    - iv. ¿Has organizado sistemáticamente estos datos de algún modo, ej., por hora o día?
    - v. ¿Hay restricciones, preocupaciones, o desafíos de algún tipo con estos datos?
    - vi. ¿Cómo has tratado con la información faltante?
    - vii. ¿Que términos de búsqueda fueron usados, que hashtags fueron seguidos? ¿En qué idiomas?
- **¿Qué métodos has usado para extraer los resultados de los datos recogidos?**
  - **b. Procesamiento y gestión de los datos**
    - i. ¿Cuál fue el proceso de traducción?, si es aplicable.
    - ii. ¿Que software fue usado?
    - iii. ¿Cuál fue el proceso de combinación y vinculado de diferentes las fuentes de datos?
  - **c. Análisis de datos**
    - i. ¿Que software,lenguajes de programación fueron usados?
    - ii. ¿Que métodos estadísticos fueron empleados?
    - iii. ¿Cuál fue el procedimiento para tratar con la información faltante?
    - iv. ¿Cuales fueron los tipos potenciales de comprobaciones de fortaleza y análisis de sensibilidad?

Antes de llamar a los expertos... prepare sus preguntas

Los investigadores tienen una facilidad de acceso a los datos nunca antes vista. Pero muchos todavía carecen de las destrezas y la confianza para trabajar con grandes conjuntos de datos. En el campo de los derechos humanos, que esta siempre limitado en presupuesto y con una carga de trabajo excesiva, los expertos en datos se encuentran siempre bajo una particular presión para satisfacer las muchas demandas de sus colegas. Cuanto más entrenado y capacitado te encuentres para realizar este trabajo, más estrés y tiempo ahorrarás tú mismo y tus colegas.

Dicho esto, a veces necesitarás llamar a los expertos. Antes de hacer algo así, prepárate para la charla, considerando las siguientes preguntas:

- **¿Cuál es tu meta final?** Ser explícito sobre tus objetivos ayuda al experto a comprender tus requerimientos.
- **¿Que considerarías una buena ayuda?**
- **¿Estás buscando asistencia para comprender el sesgo de un conjunto de datos específico**?, ¿o soporte para analizar un flujo de datos que es nuevo para ti?, ¿o quizá confirmación de que estás bien orientado en tu camino?
- **¿Necesitas asistencia puntual o continua?** Sé realista y solicita asistencia sólo en la medida en que puedas permitírtela.
- **¿Por qué este experto?** ¿Ha trabajado antes en casos similares? ¿Fué recomendado por alguien? ¿Has considerado alternativas?

Haciendo tus deberes

Busca proyectos que hayan hecho cosas similares a lo que quieres hacer. Un buen lugar para comenzar es con los casos de estudio que encontrarás en esta colección de recursos. ¿Qué es lo que te gusta específicamente de esos proyectos en lo que respecta a su uso de fuentes de datos nuevas o emergentes? ¿Están usando nuevos tipos de datos de una forma que no has visto antes, o logran extraer nuevas conclusiones basadas en un nuevo tipo de análisis?

Busca ejemplos de proyectos similares que te gusten, y que usen los nuevos tipos de datos de la forma particular que deseas. Una vez los encuentres, anota la fecha en la que fueron creados, y seleccione los elementos que encuentras particularmente inspiradores o que sean particularmente relevantes para tu trabajo. Una vez tengas una lista de proyectos, contacta con algunos de los investigadores involucrados en ellos y comprueba si tienen tiempo para una llamada rápida contigo. Sé realista: aunque un proyecto concreto podría parecer muy simple desde fuera, puede haber implicado más trabajo entre bambalinas de lo que podrías percibir.

Permanece crítico

Aunque te plantee dudas, todavía posees la mayor pericia en tu contexto específico. Si alguien trata de decirte que algo *siempre* o *nunca* es correcto, y estás en desacuerdo, confía en tu instinto.

Especialmente cuando comience a haber dinero de por medio, recoge múltiples opiniones sobre cuál sería la mejor opción para tí. Los proveedores de software, tanto si están motivados por el beneficio económico o limitados por una preferencia hacia sus propios productos, puede que no te proporcionen la mejor recomendación. Considera utilizar Software Libre y de Código Abierto (FOSS, por sus siglas en inglés), eligiendo el que sea más seguro y menos oneroso en general, siempre que sea posible.

CONCLUSIÓN

Hay varias organizaciones e individuos que están usando estas técnicas para extender los límites en el reporte y defencsa de los derechos humanos, de nuevas y excitantes maneras. Muchos de ellos han sido poderosas fuentes de inspiración para esta guía y para nuestro trabajo colectivo conjunto al permitirnos dar un vistazo de lo que existe en las fronteras del uso de datos para la documentación de situaciones de derechos humanos.

Grupos como ***Forensic Architecture***, que han realizado proyectos que usan técnicas de modelado de datos para proyectar lo que ocurrió en el pasado en base a piezas limitadas de información que perduran después del hecho; como el modelado en 3D del entorno alrededor de un ***barco en el Mediterráneo***, que fue dejado a la deriva después de que ningún país se hiciera cargo de él. Produjeron un informe que fue la base para varias reclamos legales en curso que se han iniciado contra estados miembros de la OTAN.

O ***Bellingcat***, una red de periodistas ciudadanos de investigación que usan información públicamente disponible, incluyendo datos de las redes sociales, y más generalmente Inteligencia de Código Abierto (OSINT), para investigar violaciones de los derechos humanos y otros eventos. El trabajo del fundador de Bellingcat, Elliot Higgings, en 2013, investigando el ***ataque con armas químicas sobre Ghouta, Siria***, en agosto de ese año, ayudó a probar que el perpetrador del ataque, casi con total certeza, fue el régimen de Bashar al-Assad. Han producido una fantástica colección de recursos en línea, que incluye ***casos de estudio*** y tutoriales.

Los expertos en estadísticas del Human Rights Data Analysis Group (HRDAG) han usado técnicas innovadoras para estimar de forma precisa las víctimas civiles de la guerra en varios países, siendo pioneros en la técnica llamada Multiple Systems Estimation (estimación de sistemas múltiples). Entre otros éxitos, su fundador ***Patrick Ball, ha testificado en la Corte Suprema de Justicia de Guatemala***contra el anterior jefe del estado, el General José Efraín Ríos Montt, que fue encontrado culpable de genocidio y crímenes contra la humanidad.

En lo que respecta a la verificación, individuos y organizaciones están haciendo sus procesos más transparentes. Herramientas como ***Checkdesk***, ***Github*** y ***Jupyter Notebooks*** habilitan a la gente común a documentar públicamente sus procesos y conclusiones, incrementar la credibilidad, y permitir a cualquiera seguirles y aprender de ellos. Además abren la investigación a un nuevo grado de escrutinio, más allá del de la documentación de situaciones de derechos humanos tradicional.

El futuro es nuestro y el momento es ahora

Entre tus destrezas en derechos humanos y la información en esta guía, tienes todo lo que necesitas para ponderar el valor de diferentes datos para tu trabajo, y comenzar a usarlos.

Las consideraciones, valoraciones, y usos descritos están enraizados en prácticas con las que ya estás familiarizado—como aquellas que giran en torno a ética, seguridad, y verificación.

Desarrollar la capacidad de evaluar de forma crítica y comprender qué es lo que las nuevas herramientas y plataformas te permiten hacer y cómo, continúa siendo mucho más importante que centrarse en herramientas específicas. Estar al tanto de lo que las herramientas hacen, los sesgos dentro de los datos que recibes y con los que trabajas, y, sobre todo, ocuparte de los datos de forma responsable, es tan importante como siempre.

En el momento en que se está escribiendo esto, proyectos como los discutidos previamente están lejos de ser la norma. Hablando en general, los investigadores en derechos humanos todavía usan las mismas técnicas que han estado usando durante décadas.

Los datos disponibles continuarán creciendo y se volverán más accesibles. El costo de esos datos así como los costos de las tecnologías asociadas continuarán reduciéndose. Aunque la curva de aprendizaje a veces puede ser abrupta, emplear estas técnicas es primordial para el trabajo en derechos humanos de hoy y del mañana.

RECURSOS Y LECTURA ADICIONAL

Aproveche al máximo las organizaciones y recursos que trabajan sobre el terreno. Organizaciones como ***The Engine Room*** proporcionan soporte técnico para entidades que quieren usar tecnología y datos de forma más estratégica en sus trabajos, y la ***comunidad de Responsible Data*** es un buen lugar para buscar consejo sobre desafíos éticos, legales o de privacidad, que surgen del uso de datos en contextos nuevos y diferentes. Grupos como el ***Tactical Technology Collective*** proporcionan orientación sobre el uso de la información para la defensa de derechos, como el libro ***Visualising Information for Advocacy*** (visualizar información para el proselitismo). ***School of Data*** alberga una fuerte comunidad que trabaja en la ayuda a grupos y periodistas de la sociedad civil a usar datos para contar historias. Sus cursos en línea cubren todo, desde el filtrado inicial hasta el análisis y visualización de los datos. Si quieres apoyo para configurar y usar bases de datos en tu proceso de documentación, echa un vistazo a ***Benetech***, o ***HURIDOCS***.

Para enlaces a guías más detalladas y recursos visita: ***https://engn.it/datnav***

Datos de redes sociales

Citizen Evidence Lab ***https://citizenevidence.org***

First Draft News ***https://firstdraftnews.com***

Citizen Media Research and Verification: Un marco analítico para los profesionales en Derechos Humanos ***http://www.cghr.polis.cam.ac.uk/publications/cghr-practitioner-papers-series/paper-1***

WITNESS ***https://lab.witness.org***

Normas éticas para el uso de vídeo de testigos ***https://lab.witness.org/announcing-witness-ethical-guidelines-for-using-eyewitness-footage-in-human-rights/***

Datos presupuestarios para derechos humanos

Center for Economic and Social Rights (2015), Defending Dignity: un manual para instituciones nacionales de Derechos Humanos sobre el monitoreo de los derechos económicos, sociales y culturales.

International Budget Partnership (2010), Guía para el trabajo sobre impuestos para ONGs (A Guide to Tax Work for NGOs)

Christian Aid (2011), Tax Justice Advocacy: A Toolkit for Civil Society

Fundar and International Budget Partnership (2004), Dignity Counts:una guía para el análisis presupuestario para mejorar los Derechos Humanos.

International Budget Partnership (2014), Article 2 and Governments' Budgets

OHCHR (2010), Human Rights in Budget Monitoring, Analysis and Advocacy: Training Guide

International Budget Partnership (2008),

Our Money, Our Responsibility: A Citizens' Guide to Monitoring Government Expenditures

Hakikazi Catalyst (2006), Follow the Money:

A Resource Book for Trainers on Public Expenditure Tracking in Tanzania International Budget Partnership

Open Knowledge Foundation, Open Spending Handbook, disponible en: ***http://community.openspending.org/research/handbook/***

Hoy está, manaña quizás: preservando vídeos y fotos en línea

To scrape or no not to scrape ***http://www.storybench.org/to-scrape-or-not-to-scrape-the-technical-and-ethical-challenges-of-collecting-data-off-the-web***/

Best practices in scraping: from ethics to techniques ***https://goo.gl/hovkap***

Chilling Effects ***https://lumendatabase.org–database*** que recopila y analiza quejas y peticiones legales de eliminación de materiales en línea incluyendo vídeos; Google Transparency Report (informe de transparencia de Google) coopera abiertamente con esta documentación ***https://www.google.com/transparencyreport/removals/copyright/faq/#chilling_effects***

Takedown Project ***http://takedownproject.org*** – asociado del proyecto Lumen; es un esfuerzo para movilizar a la comunidad investigadora para explorar cómo operan los procedimientos de notificación y desmantelamiento en EEUU, Europa, y otros países, y cómo estos resuelven los conflictos entre copyright y libertad de expresión

La Electronic Frontier Foundation tiene una guía y diagramas útiles sobre políticas de remoción de contenido de YouTube, y cómo desafiarlas ***https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals***

Conoce más acerca de cómo se usan los satélites para exponer abusos de derechos humanos ***https://www.theguardian.com/global-development-professionals-network/2016/apr/04/how-satellites-are-being-used-to-expose-human-rights-abuses***

Guía de introducción a los satélites y el análisis de imagen satelitales ***http://landscape.satsummit.io***

Como crear un deslizador de imágenes yuxtapuestas para antes/después: ***https://juxtapose.knightlab.com/#create-new***

Inspírate en la sección Seeing From Above (ver desde arriba) del programa Exposing the Invisible del Tactital Technology Collective, que destaca casos de uso de imágenes aéreas en distintos contextos, con entrevistas, comentarios, y guías paso a paso (how-tos) ***https://exposingtheinvisible.org***

Guías avanzadas sobre el uso de imágenes satelitales para el trabajo en derechos humanos: Monitoring Border Conflicts with Satellite Imagery: A Handbook for Practitioners ***http://www.aaas.org/report/monitoring-border-conflicts-satellite-imagery-handbook-practitioners***, Satellite Imagery Interpretation Guide: Intentional Burning of Tukuls ***http://hhi.harvard.edu/publications/satellite-imagery-interpretation-guide-intentional-burning-tukuls***

Como se ve desde el cielo: satélites y drones

Vídeos de drones relevantes para los derechos humanos ***https://www.youtube.com/playlist?list=PLRK6YeiwsEtmkkCikDM8mKSHuo9VDiE_0***

New Technologies for Property Rights, Human Rights, and Global Development ***http://drones.newamerica.org/primer/DronesAndAerialObservation.pdf***

iRevolutions ***https://irevolutions.org/category/dronesuavs/***

Unmanned Aerial Vehicles in Humanitarian Response ***https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf***

Riesgos de seguridad de la vida real

New Tactics for Human Rights Activism ha recopilado una útil lista de consideraciones y herramientas para protección y auto-preservación de profesionales de la defensa de los derechos humanos ***https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders***

Privacy, Responsibility, and Human Rights Activism ***https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders***

Towards Holistic Security for Rights Activists ***https://holistic-security.tacticaltech.org***

Protecting Journalism Sources in the Digital Age, de la UNESCO, contiene muchos consejos que también se aplican a los investigadores en derechos humanos que quieren proteger sus contactos ***http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/Themes/Freedom_of_expression/safety_of_journalists/Protecting_Journalism_Sources_in_Digital_Age_UNESCO_Flye.pdf***

¿Son seguras sus herramientas digitales?

"Security in a Box" (caja de herramientas de seguridad) del Tactical Technology Colective

Hacer copias de seguridad de tu software: *https://securityinabox.org/en/guide/backup*

Almacenamiento seguro de archivos: *https://securityinabox.org/en/guide/secure-file-storage*

Destruir información: *https://securityinabox.org/en/guide/destroy-sensitive-information*

Secure app scorecard: *https://www.eff.org/secure-messaging-scorecard*

The Responsible Data Forum's Handbook of the Modern Development Specialist *https://responsibledata.io/resources/handbook/chapters/chapter-01-designing-a-project.html*

Setting Up the Data Infrastructure: *https://responsibledata.io/resources/handbook/chapters/chapter-02-managing-data.html*

Una Introducción al Modelo de Amenaza: *https://ssd.eff.org/en/module/introduction-threat-modeling*

Threat Modeling for Campaigners and Activists *http://www.mobilisationlab.org/threat-modeling-for-campaigners-and-activists*

Guía de Auto-Protección contra la Vigilancia de la EFF: *https://ssd.eff.org/*

Holistic Security Manual *https://holistic-security.tacticaltech.org*

Cómo encuadrar tu investigación

Human Rights Data Analysis Group (HRDAG): Core Concepts *https://hrdag.org/coreconcepts*/

Responsible Data Forum: Recognising uncertainty in statistics (Brian Root, HRW) *https://responsibledata.io/reflection-stories/uncertainty-statistics/*

Kelly Greenhill: Nigeria's Countless Casualties Foreign Affairs *https://www.foreignaffairs.com/articles/africa/2015-02-09/nigerias-countless-casualties*,Tufts University *http://as.tufts.edu/politicalscience/sites/all/themes/asbase/assets/documents/newsEvents/2015febForeignAffairsGreenhill.pdf*

Selected HRDAG publications on selection bias *https://hrdag.org/publications/big-data-selection-bias-and-the-statistical-patterns-of-mortality-in-conflict/*

Publicaciones escogidas de HRDAG sobre sesgo de selección *https://hrdag.org/wp-content/uploads/2013/02/Gohdes_Convenience-Samples.pdf*

https://hrdag.org/wp-content/uploads/2013/02/results-paper.pdf

https://targetedthreats.net/

https://hrdag.org/wp-content/uploads/2015/07/HRDAG-SY-UpdatedReportAug2014.pdf

https://hrdag.org/wp-content/uploads/2013/02/uv-estimates-paper_2012-11.pdf

https://hrdag.org/wp-content/uploads/2013/02/Benetech-TRC-descriptives-final.pdf

https://hrdag.org/wp-content/uploads/2013/02/Benetech-Report-to-CAVR.pdf

https://hrdag.org/wp-content/uploads/2013/02/State-Violence-in-Chad.pdf

Antes de llamar a los expertos... prepare sus preguntas

Video: WITNESS *https://witness.org*/

Métodos estadísticos:
the Human Rights Data Analysis Group (HRDAG)
https://hrdag.org

Integrar + comprender los datos y la tecnología de forma estratégica:
The Engine Room *https://theengineroom.org*

Recogida de datos de forma segura + necesidades de software // Seguridad digital:
Benetech *http://www.benetech.org*

Gestión de documentos:
Huridocs *https://www.huridocs.org*

Audiovisuales de Eyewitness:
the Eyewitness Media Hub
http://www.eyewitnessmediahub.com

Tactical Technology Collective
https://tacticaltech.org

Redes/comunidades:
New Tactics in Human Rights
https://www.newtactics.org

Open Government Partnership
http://www.opengovpartnership.org