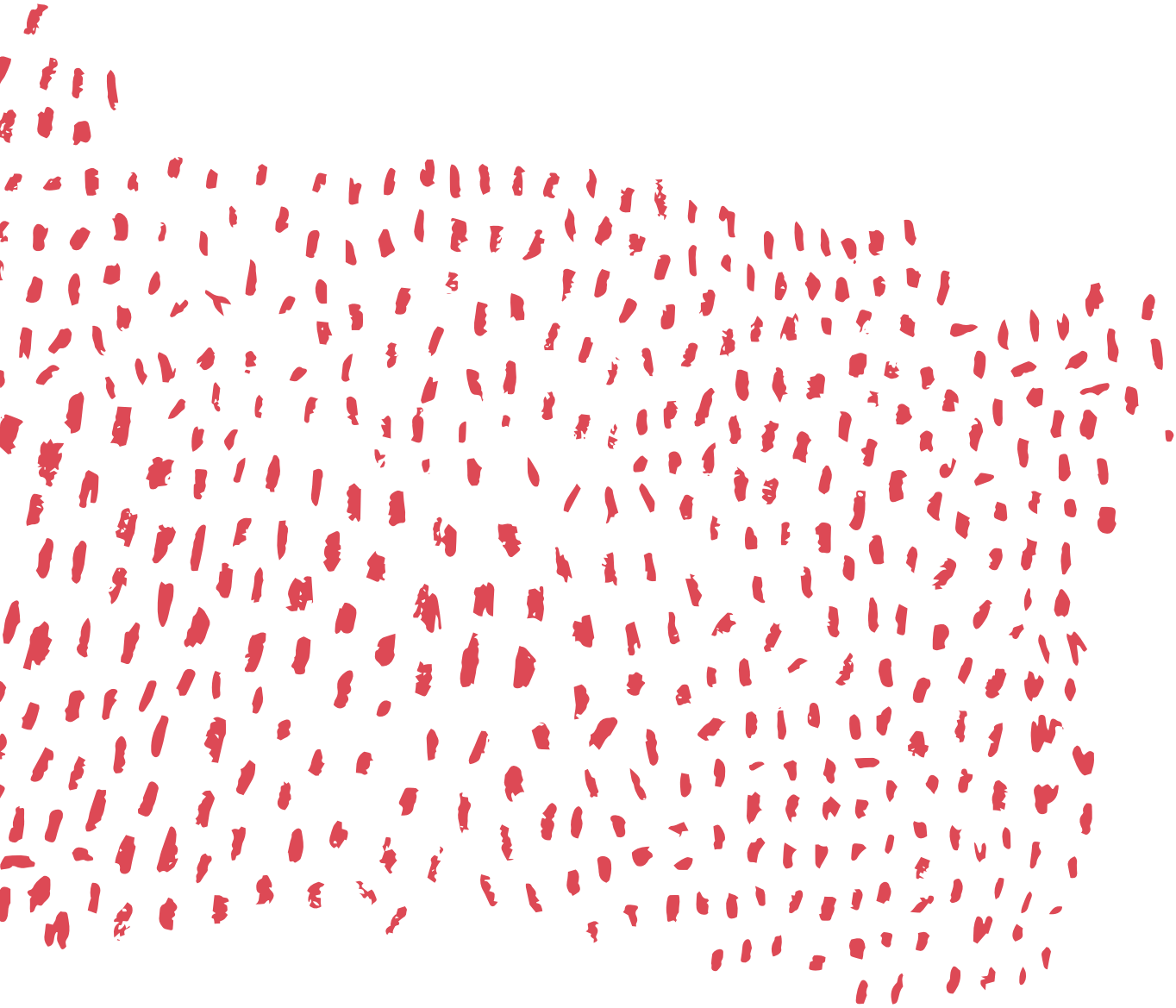
DATNAV

Cómo navegar entre datos digitales para la investigación en derechos humanos

THE ENGINE ROOM

benetech
TECHNOLOGY SERVING HUMANITY

AMNESTY INTERNATIONAL



CENTER FOR ECONOMIC AND SOCIAL RIGHTS

CG+HR 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

Contribuidores

Damos las gracias a los siguientes contribuidores al **sprint de escritura**:

- Allison Corkery, Center for Economic and Social Rights
- Sam Dubberley, Eyewitness Media Hub y el proyecto Human Rights, Big Data and Technology de la Universidad of Essex
- Scott Edwards, Amnistía Internacional
- Lisa Gutermuth
- Danna Ingleton, Amnistía Internacional
- Christoph Koettl, Amnistía Internacional
- Jule Krüger, Human Rights Data Analysis Group (HRDAG)
- Chris Michael, Collaborations for Change
- Ella McPherson, Department of Sociology y Centre of Governance and Human Rights de la Universidad de Cambridge
- Shabnam Mojtahedi, Syrian Justice and Accountability Center
- 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 en llamamientos de la comunidad, o entrevistados en la fase temprana de este proyecto:

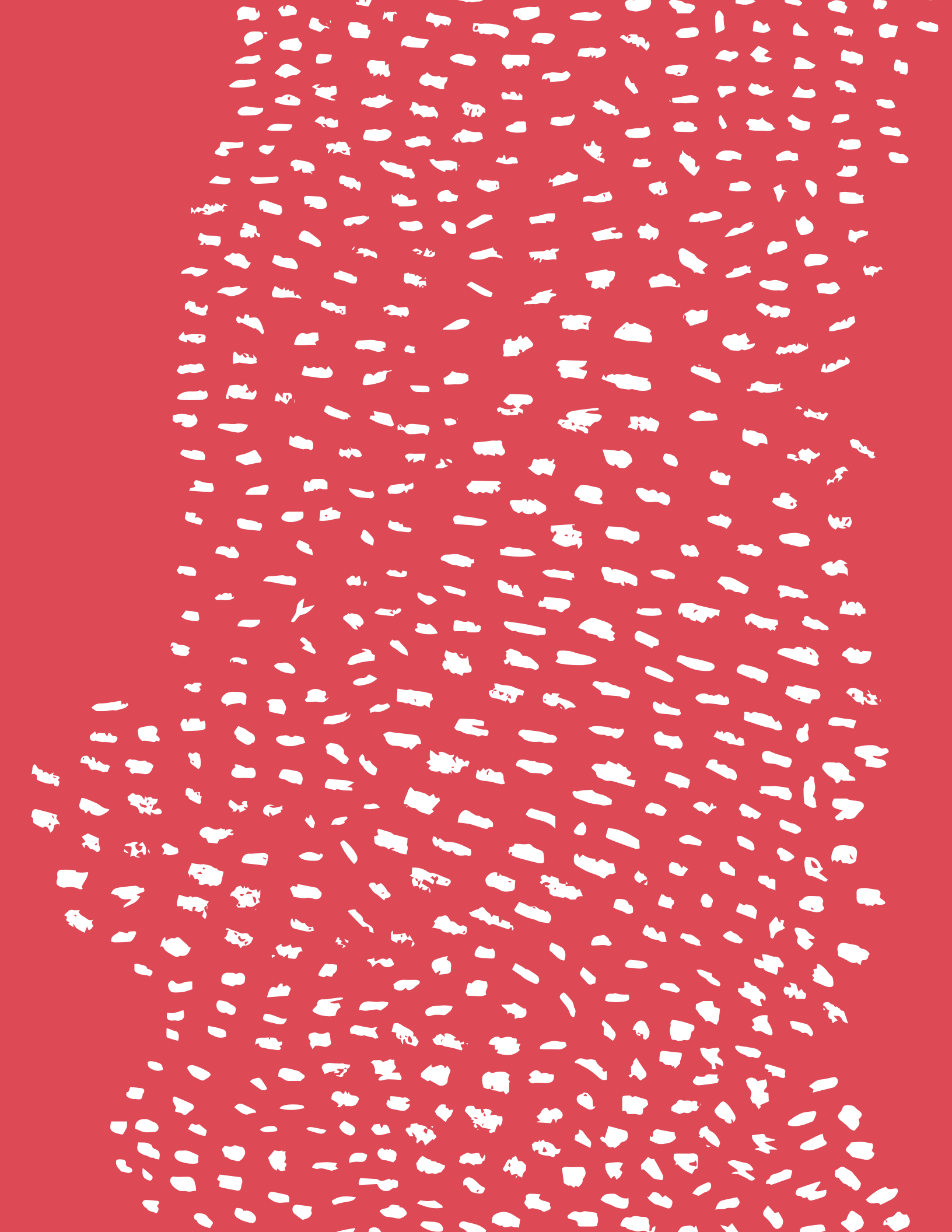
- Kristin Antin, HURIDOCS
- Jay Aronson, Center for Human Rights Science de la Universidad Carnegie Mellon
- Patrick Ball, HRDAG
- Alexis Bautista, Migrant Forum in Asia
- Anh Bui, Benetech
- Neil Blazevic, East and Horn of Africa Human Rights Defenders Project
- Laura Carter, Amnistía Internacional
- Kristy Crabtree, International Resue 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, Syria Justice and Accountability Center
- John Emerson, NYU Center for Human Rights and Global Justice
- Wael Eskandar
- Emmanuel Freudenthal
- Niamh Gibbons, Harvard Humanitarian Initiative
- 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, Amnistía Internacional
- 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 de la Universidad de Columbia
- Robin Pierro, European Inter-University Centre for Human Rights and Democratization
- Enrique Piraces, RightsLab
- Vanya Rakesh, CIS India
- Vijay Rao, Syria Justice and Accountability Center
- 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

Cubierta: Lynne Stuart.
Diseño gráfico por Federico Pinci.

Publicado por primera vez en junio de 2016

CONTENIDOS



Iniciarse

INTRODUCCIÓN

Desde vídeos en línea de violaciones de derechos, a imágenes de satélite de degradación ambiental, o relatos de testigos presenciales diseminados en medios sociales, tenemos acceso a más datos relevantes hoy que nunca antes. Cuando se usan con responsabilidad, estos datos pueden ayudar a los profesionales de la defensa de los derechos humanos en un tribunal, cuando trabajan con gobiernos y periodistas, y en la documentación del registro histórico.

Adquirir, propagar y almacenar datos digitales también se está volviendo cada vez más asequible. En tanto continúan reduciéndose los costes 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 recogida y administración de datos en el trabajo del día a día de la investigación y documentación en derechos humanos, puede ser desafiante, incluso apabullante, para individuos y organizaciones. Esta guía está diseñada para ayudarle a explorar e integrar nuevas formas de datos en su trabajo en derechos humanos.

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 no hemos encontrado nada. ¿Por qué?

Principalmente, los investigadores en derechos humanos parecían estar abrumados por las posibilidades. Frente a recursos limitados, no sabiendo cómo iniciarse o si merecería la pena, la mayoría de las personas con las que hablamos se contuvieron incluso de intentar reforzar su trabajo con datos digitales.

Para dar apoyo a todos los que trabajan en el campo de los derechos humanos para navegar por este entorno complejo, hemos reunido a un grupo de 16 investigadores y expertos técnicos en un castillo en el exterior 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 USTED

Asumimos que sabe cómo realizar investigación en derechos humanos, pero deseamos expandir su conocimiento de cómo usar los datos digitales y medios en línea para propósitos de documentación.

Esta es una introducción amplia que le pondrá en el buen camino para formular sus propias preguntas y buscar sus propias soluciones. Pretendemos inspirar el pensamiento crítico, en lugar de ser prescriptivos en cuanto a qué software, dispositivos, o plataformas específicas se deben usar, ya que estas evolucionan constantemente.

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

Imaginamos que es un investigador en derechos humanos, periodista, estudiante, diseñador de políticas o filántropo, que quiere...

› Impulsar la investigación y documentación tradicionales (entrevistas, encuestas, y hojas de cálculo) aprendiendo a incorporar datos digitales.
› Crear conocimiento y pericia anticipándose a la próxima emergencia, para evitar el recopilado de datos como reacción mientras se produce un evento o violación de derechos.
› Comprender las oportunidades, límites y riesgos de los datos digitales, además de cuándo y cómo buscar consejo experto para ayudarle a alcanzar sus metas.
› Superar el miedo a los datos y la tecnología digital, que ya son de uso intensivo entre sus colegas. Con mejores herramientas, usted sabe que puede ser más eficiente.

Iniciarse

NUEVAS POSIBILIDADES CON DATOS DIGITALES

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

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

Hoy, millones de personas tienen la capacidad de capturar fotografías o vídeo de alta resolución con dispositivos que caben en sus bolsillos. Pueden compartir con facilidad lo que han capturado con audiencias cercanas y lejanas, protegiendo enormemente sus observaciones a lo largo del espacio y el tiempo, al margen de fronteras e idioma.

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

Comparado con hace sólo unos pocos años, hay inmensas posibilidades que parten de tener abundantes datos de numerosas fuentes para respaldar el trabajo en defensa de los derechos humanos. Los datos digitales pueden sustentar la documentación de situaciones de derechos humanos en profundidad, amplitud, precisión, y de forma eficiente.

Primero, pueden ofrecer una nueva fuente de corroboración de evidencias para la documentación tradicional de eventos específicos. Las violaciones de los derechos humanos a menudo se tipifican por un evento. Armados con nuevas fuentes de datos, la cantidad de detalles que pueden ser revelados acerca de un evento en particular 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 cartografiar tendencias y patrones que ayudan a sacar a relucir más disfunciones sistémicas.

Redefinición de métodos tradicionales

La documentación de situaciones de derechos humanos tradicionalmente ha implicado entrevistar a víctimas y testigos, y reunir evidencias corroboradoras. 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 (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 tome la iniciativa. Esto puede consistir en hacer *algo inconcreto* o en hacer *algo de forma distinta*. Un gran número de violaciones de los derechos humanos —en particular las de derechos económicos, sociales, y culturales — entran en esta segunda categoría. Son ejemplos el tráfico de seres humanos, la explotación laboral, la brutalidad policial, la malnutrición, 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 luchan por revelar. Estas disfunciones pueden ser causadas por un gran número de actores y factores, que hacen 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

Hacer un mejor uso de datos de Siria para documentar violaciones de derechos

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

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

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

Foto: *Damasco*, 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 de satélite probablemente podrían ayudar a localizar un enterramiento, 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 de satélite mostraron verazmente tierra removida en el punto identificado.

El hallazgo de un enterramiento masivo vía satélite 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.

Para que cualquier dato sea útil para la documentación de situaciones de derechos humanos, ha de poder ver el lugar de donde vino, cuándo fue creado, quién lo creó, y por qué. Lugar, Hora, Persona, Motivación.

¿CUÁNDO DEBE USAR DATOS DIGITALES?

Si está más acostumbrado a la investigación y documentación tradicionales, puede ser desalentador dedicarse a evaluar si los datos digitales o el contenido de medios sociales son merecedores de su atención.

Esta sección lista siete preguntas para ayudarle a ponderar el valor neto de nuevos tipos de datos en el contexto particular de su investigación. ¿Serán de verdad de ayuda? Necesitamos sopesar constantemente los pros y contras, incluyendo los costes, ahorros, y ***riesgos de hacer un mal manejo de los datos***. Por ejemplo, el riesgo de ser vigilado puede hacer que la recopilación de datos digitales pase inadvertida en algunas configuraciones, o puede que sólo tenga acceso a algunas poblaciones pero no a otras sesgando los resultados de su 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 usted y su equipo pueden recopilarlos y manejarlos de forma efectiva.

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

1. ¿Ayudarían los datos digitales a responder de verdad a sus preguntas? ¿Cuáles son los pros y contras de la fuente o medio en particular? ¿Qué podría aprender de pasados usos de tecnología similar?
2. ¿Qué fuentes es probable que estén recogiendo o capturando el tipo de información que necesita? ¿Cuál es el contexto en que esta se viene produciendo y utilizando? ¿Serán receptivas a este tipo de datos las personas u organizaciones hacia las que se orienta su trabajo?
3. ¿Con qué facilidad se integrarán las nuevas formas de datos en su dinámica de trabajo? ¿Tiene realmente el tiempo y el dinero para recopilar, almacenar, analizar, y especialmente, para verificar estos datos? ¿Puede cualquiera de su equipo encargarse con comodidad de la tecnología?
4. ¿Quién posee o controla los datos que va 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? ¿Tiene 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? ¿Las conclusiones basadas en los datos reforzarían las desigualdades, estereotipos o puntos ciegos?
6. ¿Son suficientemente robustos los protocolos organizativos para confidencialidad y seguridad en la comunicación digital y manejo de datos, para afrontar los riesgos para usted, sus asociados, y sus fuentes? ¿Se actualizan con suficiente frecuencia las herramientas y procesos de seguridad?
7. ¿Tiene medidas de contingencia en su emplazamiento para evitar o afrontar cualquier trauma secundario producido por ver contenidos digitales perturbantes que usted o sus asociados puedan experimentar a nivel personal o de 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?

Desean investigar alegaciones sobre denegación de acceso a atención sanitaria a refugiados en tránsito, y están considerando usar fotografías de satélite para cartografiar rutas de viaje recientes, y contenido de medios sociales para buscar testimonios y entrevistar sujetos. Tienen un presupuesto muy limitado y no han usado antes este tipo de datos, pero saben que la mayoría de los refugiados tienen teléfonos móviles y usan medios sociales para compartir información. Su mayor preocupación es que los datos de geolocalización puedan acabar en manos de comités locales de vigilantes que ataquen a los inmigrantes. De hecho, a causa de los grupos de vigilantes, 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?

Deciden buscar acceso a grupos cerrados de medios sociales a través de sus contactos, y hacer de la seguridad de todos aquellos con los que se comuniquen en línea su máxima prioridad. Consultan con individuos y grupos acerca de las denegaciones de acceso a atención sanitaria. Por ahora, renuncian a usar fotos aéreas.

CUESTIÓN A INVESTIGAR:
¿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. Ha habido informes de violación del 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 DE CENTROS MÉDICOS [c]
- DATOS DE MEDIOS SOCIALES 'CERRADOS' [d]
- INFORMACIÓN AÉREA NO-SATELITAL
- INFORMACIÓN PRESUPUESTARIA DEL GOBIERNO [e]
- INFORMACIÓN DE DATOS DE MEDIOS SOCIALES
- DATOS DE LA DERIVA OCEÁNICA [f]

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

b Como ciudadanos informando de mapas de incidentes relacionados con refugiados en el punto de entrada.

c Estructuras que proporcionan apoyo médico a refugiados.

d 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 U otros factores que pueden afectar el movimiento de refugiados.

Escenario

Rastrear censura en Internet | ¿Debemos usar datos digitales?

Está trabajando en un país donde el gobierno es conocido por clausurar Internet durante protestas y turbulencias sociales, y desea documentar esto. Descubre que puede acceder en línea a los registros de ***interrupción de servicio de Google***, que le permitirían identificar probables episodios de inactividad cuyas referencias pueden cruzarse con otras fuentes de datos. Sin embargo, el gobierno está experimentado en vigilancia digital y de Internet, y podría rastrear la actividad de su navegador y su historial de búsqueda hasta dar con usted, identificándole como un activista en defensa de los derechos humanos.

¿Qué hacer?

Dado el historial de vigilancia del gobierno, su organización le ha instruido en el uso de ***VPNs (redes privadas virtuales)*** para hacer búsquedas y comunicarse en línea. Decide que puede ocultar suficientemente sus rastros digitales para realizar su investigación a pesar de los riesgos.

CUESTIÓN A INVESTIGAR:
¿Violó el gobierno del País Y la libertad de expresión y el derecho 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 del país.

VIOLACIONES DE DERECHOS EN INTERNET

TIPOS DE DATOS POTENCIALES

- REGISTROS DE LA COMPAÑÍA DE SERVICIOS DE INTERNET
- INFORMES DE MEDIOS
- REGISTROS DE DESCARGA DE NUEVAS APLICACIONES [a]
- ANÁLISIS DE VELOCIDAD DE INTERNET
- DECLARACIONES DEL SECTOR PRIVADO/ONGs [b]
- PETICIONES DE DESMANTELADO O CIERRES DEL USUARIO [c]
- ESTADÍSTICAS DE TRÁFICO EN INTERNET [d]
- MEDIOS SOCIALES
- REGISTROS TELEFÓNICOS [e]
- BLOQUEO GUBERNAMENTAL DEL ACCESO A INTERNET [f]
- DATOS DE PSIPHON

a En particular los que se consideran seguros y accesibles.

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

c Reportados por compañías de medios sociales.

d Generalmente en sitios 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, le 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. Le gustaría distribuir un SMS para realizar un sondeo preguntando si su acceso al agua está siendo limitado y dónde, pero la población ha sido objetivo de muchos programas de desarrollo en los últimos años y ha oído que está un tanto cansada de sondeos. Su ONG es joven y tiene recursos limitados.

¿Qué hacer?

Aunque el sondeo SMS le permitirá llegar a su población objetivo, el contexto puede evitar que obtenga respuestas. Dado que (1) su objetivo es una población más pobre cansada de sondeos, que (2) tendrá que pedir a cada persona que responda que pague por el mensaje de respuesta, y que (3) su ONG tiene un nombre con poco reconocimiento, se da cuenta de que esto podría ser una batalla contra los elementos. Decide pedir a un colega en una ONG bien establecida que le presente a un líder comunitario para que pueda explicarle el proyecto, pedir la contribución de la comunidad en el diseño de la encuesta, y resolver cómo difundir la información de su proyecto en marcha de vuelta hacia la comunidad.

CUESTIÓN A INVESTIGAR:
¿Es responsable FPower de la contaminación del suministro de agua?

En el País X hay altos niveles de malnutrición 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

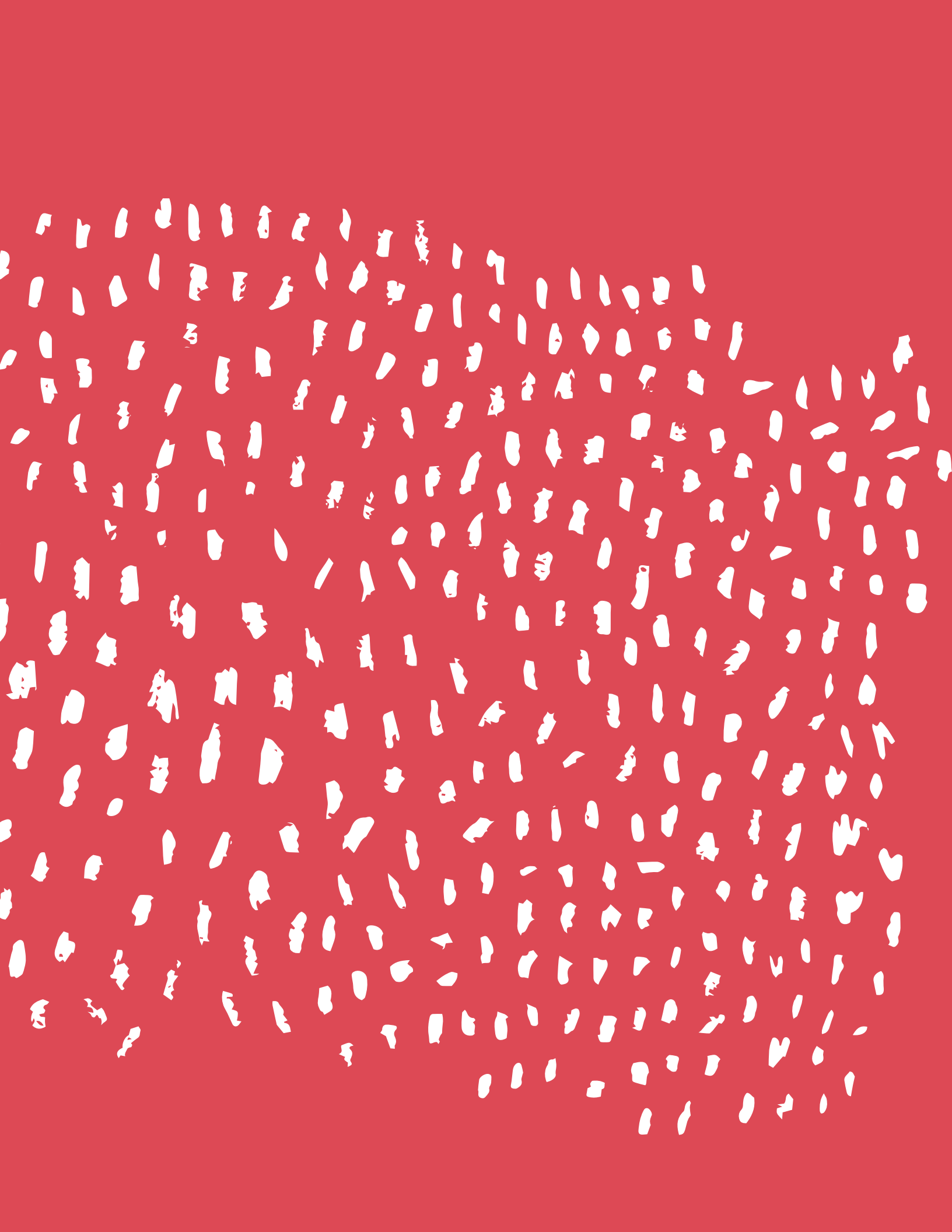
- ESTADÍSTICAS NACIONALES DE SALUD
- FOTOGRAFÍAS O IMÁGENES DE SATÉLITE [a]
- ANÁLISIS DE BÚSQUEDAS/ DATOS/ INTERNET
- DATOS DE PRESUPUESTOS [b]
- INFORMACIÓN DE OPERACIONES Y LOCALIZACIÓN DEL NEGOCIO
- DATOS DE ENTREGA DEL SERVICIO [c]
- SONDEO SMS SOBRE CONSUMO DE CALORÍAS
- ANÁLISIS DE CONTAMINACIÓN DEL AGUA
- SUPERPOSICIÓN DE DATOS GEOGRÁFICOS Y TEMPORALES

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

OBTENER APOYO ORGANIZATIVO

Incluso donde hay apetito por el cambio, largas jornadas de trabajo y presupuestos ajustados, individuos y organizaciones pueden permanecer 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 tiene **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 están trabajando con datos digitales, pero muchas lo hacen sin invertir en alfabetización digital. No desarrollar las destrezas internas necesarias para su organización pone la relevancia de su trabajo en riesgo.
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. La investigación muestra que los empleados valoran las nuevas oportunidades de capacitación en el trabajo sólo 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 utilizar nuevas herramientas ayuda a atraer a los mejores profesionales en ese campo.
5. **Impacto**: Usar los nuevos datos de forma eficiente puede mejorar los resultados y permitir una mejor monitorización de violaciones de derechos humanos.
6. **Financiación**: Los donantes son proclives a vincular nuevos llamamientos para propuestas de financiación con datos digitales y su uso en información de derechos humanos.
7. **Impulso de marca**: Hacen parecer a una marca ágil, visionaria, y deseosa de implicarse en nuevos desarrollos.
8. **Misión**: La misión es monitorizar, informar y elevar la percepción de las violaciones de derechos humanos. Usados debidamente, los datos digitales permiten a las organizaciones hacer esto de mejor modo.
9. **Charlas en almuerzos para el personal**: Invite a alguien que trabaje con éxito con datos digitales a dar una charla acerca de lo que están haciendo.
10. **Construir redes entre semejantes**: 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 fichero (como un documento word, un PDF, una imagen, un fichero de música, etc.) que se guardan dentro del propio fichero, ocultos de la vista.

Esta información puede incluir la fecha y hora en que fue creado un fichero, el nombre de usuario de las personas que lo crearon o editaron, información acerca del dispositivo que lo creó, y otros tipos de información. En otras palabras, los metadatos en un fichero podrían revelar quién creó un fichero. Esta información es generada automáticamente por dispositivos como cámaras, computadoras, y teléfonos, pero también puede ser editada y manipulada por quienes saben cómo. Esto puede ser algo bueno, si quiere que la información sea privada al compartir ficheros, pero los riesgos son obvios si está tratando con verificación de información sensible de derechos humanos.

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

Los formatos de fichero 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 antes descrita, e incluso una miniatura de la imagen original.

Otros ficheros, como documentos de texto, también incluyen metadatos. Podrían referirse al 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.

Limpiar a fondo los metadatos

En algunos casos puede que quiera eliminar metadatos de los ficheros 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 usted 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 ficheros. Aunque no todos los metadatos se pueden eliminar —como el tamaño del fichero, las dimensiones de una imagen, o la hora de la última modificación— los metadatos relativos a quién creó y editó el fichero 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*** (seguridad en un dispositivo), del Tactical Technology Collective y Frontline Defenders, tiene aún más información sobre la eliminación de metadatos.

VERIFICAR, VERIFICAR, VERIFICAR

Los datos de cualquier tipo —incluso de materiales que usted mismo recopiló— requieren verificación exhaustiva para proteger su reputación, y a las personas sobre el terreno de sufrir daño. Es importante aproximarse a cada pieza de contenido con un ojo crítico, especialmente si su deseo es que sea veraz.

También tiene que aceptar que no hay un único método de garantizar la verificación. La verificación es un proceso para proporcionarle a usted y a otros confianza en la veracidad del contenido. Debe ser tan transparente acerca de lo que no sabe como de lo que sabe, en interés de todos.

Bajo gran presión, la verificación de datos digitales en entornos de bajos recursos a menudo es una ocurrencia tardía en lugar de algo que está incorporado en los planes de investigación desde un principio. Si tiene dudas acerca de cómo verificar un tipo particular de contenido, es más seguro consultar a expertos para que le ayuden.

Los cinco pasos de la verificación

1. **¿Cómo obtuvo el contenido?**
   Piense a través de qué canales de información viajó antes de llegar a su mesa ¿Cuántas veces cambió de manos?
2. **¿Quién creó el contenido?**
   ¿Es también el creador la persona que compartió o subió el contenido en línea, o es alguna otra? Pregunte si no lo sabe.
3. **¿De dónde viene el contenido?**
   Las descripciones y metadatos se pueden falsificar fácilmente. ¿Hay marcas visibles o sonidos (como sirenas de policía o dialectos) que puedan ayudarle a verificar una ubicación?
4. **¿Cuándo fue creado el contenido?**
   No puede confiar en la marca de fecha en un fichero. ¿Hay pistas visuales como la meteorología? 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?

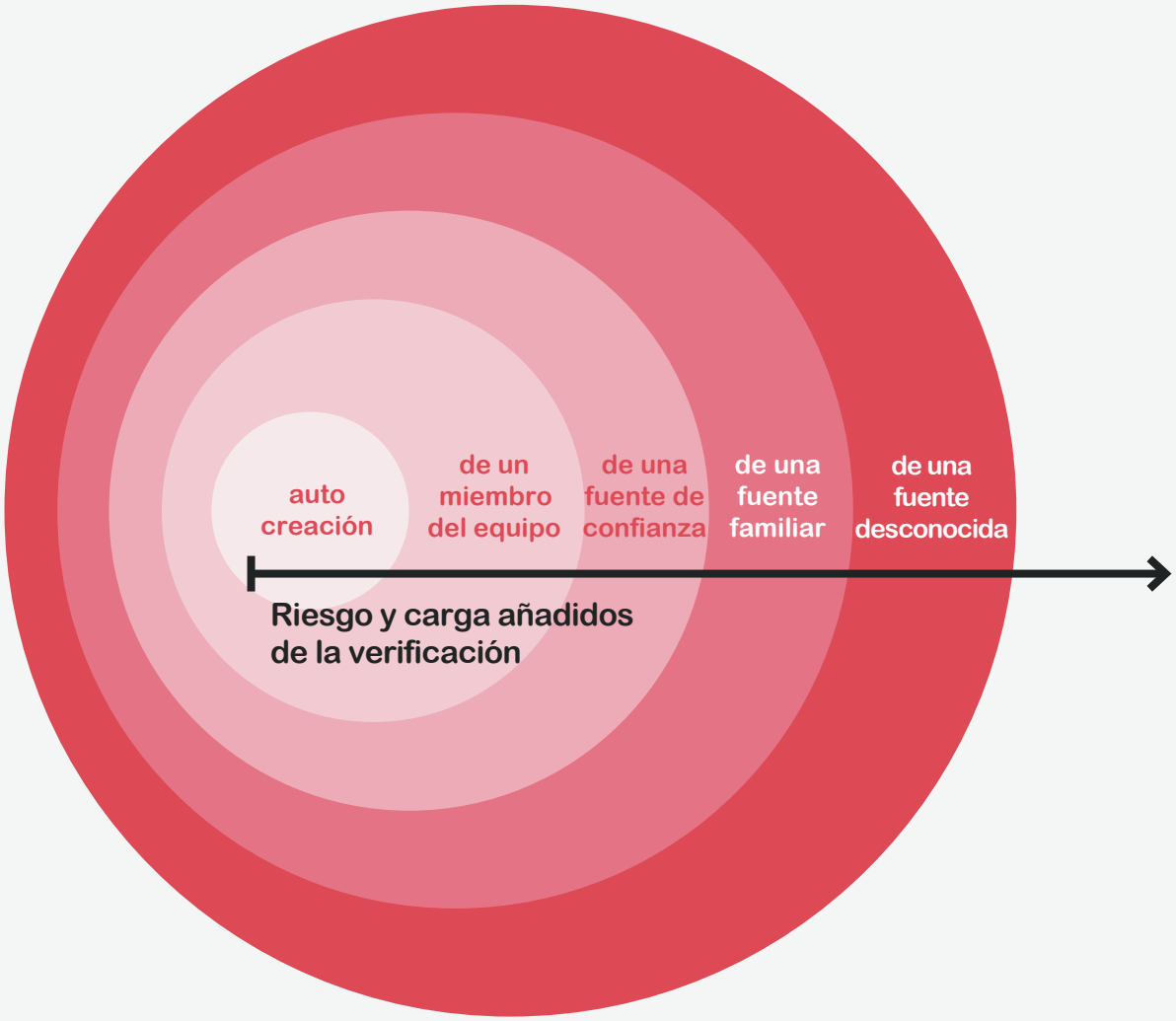
¿Por qué verificar?

Puede sonar obvio, pero a menos que trabaje con material que haya recogido usted mismo, o con sus observaciones de primera mano, es importante verificar que la información con la que está trabajando sea de hecho lo que pretende ser. Los riesgos de reputación, además de hacia los sujetos de la investigación, requieren la debida diligencia al trabajar con nuevos datos de cualquier clase.

Pasos de la verificación

La verificación es un proceso en evolución. Y el producto final raramente es definitivo. Más bien es un proceso que concede confianza en 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 ponerse a verificar la pieza de 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

Usted es un investigador en derechos humanos, y necesita 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 con usted.

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 usted, mirando en otras plataformas de medios sociales, dedujo 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 use imágenes de satélite encontradas en Google Earth para cruzar referencias de elementos prominentes visibles (edificios de oficinas, puentes peatonales, etc.).

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 accedió 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. Usa una reproducción de vídeo a cámara lenta (en YouTube o *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 busca contenidos adicionales con su motor de búsqueda regular, puede encontrar varios **otros vídeos de la misma fecha y protesta** [*https://youtu.be/sxyrP0yBBts*], que corroboran el vídeo.

Cómo verificar imágenes usando ficheros EXIF (Preguntas y Respuestas)

Todas y cada una de la fotos digitales contienen un fichero de metadatos llamado EXIF que puede identificar cuándo y dónde fue capturada una imagen. Esta información se añade al fichero en el momento en que toma la foto, sin importar el dispositivo que use. Los ficheros 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 un fichero EXIF?
Una imagen debe contener un fichero EXIF si viene directamente de la cámara fuente hasta su bandeja de entrada sin ser alterada o haber cambiado de manos. Si fue editada, todavía puede tener un fichero EXIF. Si una imagen no contiene un fichero EXIF, debe cuestionar su originalidad. Puede comprobar el 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 datos EXIF en su imagen?
La mayoría de las plataformas audiovisuales despojan las fotos de datos EXIF o crean copias de baja calidad cuando una foto es subida a su plataforma (con la excepción de los sitios web dedicados a la compartición de fotos). Si está verificando una foto proveniente de un medio social, habitualmente no encontrará datos EXIF.

¿Cómo encuentro los datos EXIF?
Si busca en línea "EXIF data viewer" (o visor de datos EXIF) verá 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 puede encontrar los datos EXIF usando aplicaciones en su computadora como Photoshop o iPhoto.

¿Se pueden manipular los datos EXIF?
Sí. Herramientas como ***Geosetter*** y otras aplicaciones de software de edición de fotos se pueden usar para falsificar datos EXIF. Esto significa que los datos EXIF sólo se deben usar como uno de muchos pasos en su 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 datos EXIF sólo le dicen el dispositivo que capturó la imagen, no saben nada acerca de lo que había realmente frente a la cámara. Incluso si el fichero EXIF coincide en fecha y ubicación, la imagen aún puede ser alguna otra distinta de la que pretende ser, por ejemplo, una foto de una foto.

En profundidad

Qué dice una foto sobre usted...

Este es el aspecto que tienen los ficheros 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 datos EXIF serán relevantes para la verificación.

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

Esto es el modelo de cámara o teléfono. Si, por ejemplo, intercambia correspondencia con una persona que ha compartido una imagen con usted, puede corroborar lo que cuentan los datos EXIF sobre la cámara usada para capturar la imagen con lo que la persona le dice acerca del dispositivo con el que la capturó. Si le habla de 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

Esto es importante para comprobar la hora a la que fue capturada una foto, pero EXIF no indica la zona horaria. Puede bien reflejar la hora local o la Hora Universal Coordinada (UTC), dependiendo del dispositivo y la configuración. Algunas marcas de cámara tiene sus propias etiquetas de metadatos como suplemento a EXIF, y pueden incluir datos de zona horaria. También hay una etiqueta EXIF no estándar para TimeZoneOffset que puede indicar la compensación de hora relativa a GMT. Muchos sitios de alojamiento de audiovisuales, como YouTube, establecen por defecto la Hora de la Costa del Pacífico (PST) si la zona horaria no está integrada en la imagen. También debe considerar si las configuraciones de fecha y hora de su dispositivo pueden haber sido incorrectas. Esto es más probable con una cámara que con un smartphone, ya que este último a menudo actualiza las configuraciones de fecha y hora automáticamente.

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 datos EXIF pueden mostrar las coordenadas GPS del lugar donde fue tomada. GPS significa Global Positioning System (sistema de posicionamiento global) —un sistema de localización por satélite. Si están disponibles, la mayoría de los visores de datos 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 (anchura y altura) son útiles de dos maneras. Primero, diferentes cámaras que producen imágenes con el mismo recuento de píxeles pueden producir imágenes con distintas dimensiones. Por ejemplo, las cámaras Fujifilm XT-2 y Leica M-D Typ 262 producen imágenes de 24 megapíxeles, pero con distintas dimensiones. Las dimensiones en píxeles de la Fujifilm XT-2 son: 6000 x 4000 píxeles. 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 su 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 sube una foto a un motor de búsqueda de imágenes y realiza una "búsqueda inversa de imagen", el motor comprueba nombres de fichero coincidentes, o imágenes similares que ya aparecen en línea. Esto puede ayudarle a determinar si una foto es lo que cree que es, si es más antigua de lo que cree, o si ha sido usada previamente en un contexto o país distinto.

1. **Encuentre el motor de búsqueda adecuado para usted.**
   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 le funciona mejor.
2. **Realice siempre dos búsquedas.**
   Cada motor de búsqueda inversa de imagen consulta una base de datos distinta, e indexa nuevas imágenes a diferente velocidad. Su imagen puede aparecer en un motor de búsqueda a la vez que no en otro.
3. **Ordene 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. **Localice referencias geográficamente.** Si trata de identificar elementos prominentes en una imagen o vídeo, un motor que permita búsquedas "similar a" es de gran ayuda, ya que están muy documentados.

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

¡Cuidado! Si su imagen no aparece en una búsqueda inversa de imagen, no significa que sea nueva. La imagen podría haber estado aparcada en un disco duro durante años.

Caso de estudio

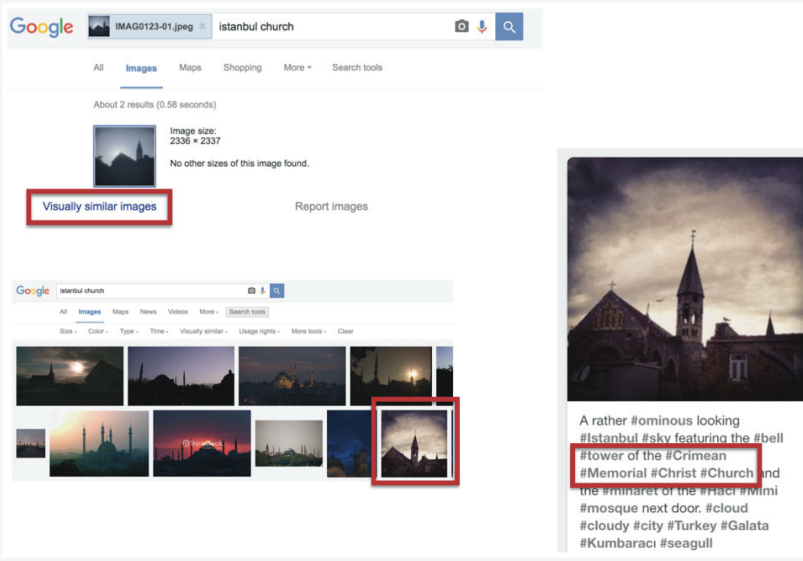
Verificar la localización de esta imagen

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 puede hacer este tipo de verificación con vídeos. Simplemente haga una captura de algún elemento prominente en un vídeo, y siga los mismos pasos.



DATOS DE MEDIOS 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 medios 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 de medios 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. Adicionalmente, la gran cantidad de contenido compartido entre múltiples plataformas puede abrumar fácilmente a los investigadores, y a veces esto supone una llamada para buscar destrezas especializadas de organización y rastreo.

Los medios sociales son muy distintos de las fuentes tradicionales, como el testimonio de un testigo presencial o la información periodística, no tanto porque la fuente original de la información a menudo no sea clara, sino porque ***la desinformación puede extenderse*** increíblemente rápido de una persona a miles. Pero al mismo tiempo, los medios 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 medios sociales permitió la reconstrucción del asesinato de un manifestante pacífico por la policía en 2015, y subsecuentemente forzó una investigación y un juicio. En ***Nigeria***, los contenidos de medios sociales jugaron un papel crucial para documentar crímenes de guerra en 2014.

Cuando los investigadores tengan más destreza en formular preguntas adaptadas a medios sociales y empleen herramientas técnicas para procesar conjuntos más grandes de datos, podrán efectuar análisis avanzados a lo largo del tiempo, para distintos lugares e 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 sensaciones" de twits rusos*** sobre la amenaza de guerra en Crimea, mostrando una oposición leve.

Iniciarse con la investigación en medios sociales

Use los medios sociales para la defensa de los derechos humanos siempre de forma segura, ética, e impactante. Necesita *descubrir, organizar, preservar* y *verificar*. El propósito de las siguientes preguntas es proporcionar orientación. Úselas en su investigación, al margen de con qué plataformas esté trabajando.

¿Qué plataformas y aplicaciones son dominantes en su país o región?
"Medios sociales" 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 su tema?
La gente se comunica usando palabras clave específicas o hashtags. Siga 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 evocador que lo que usted encuentre con la primera búsqueda que se le ocurra.

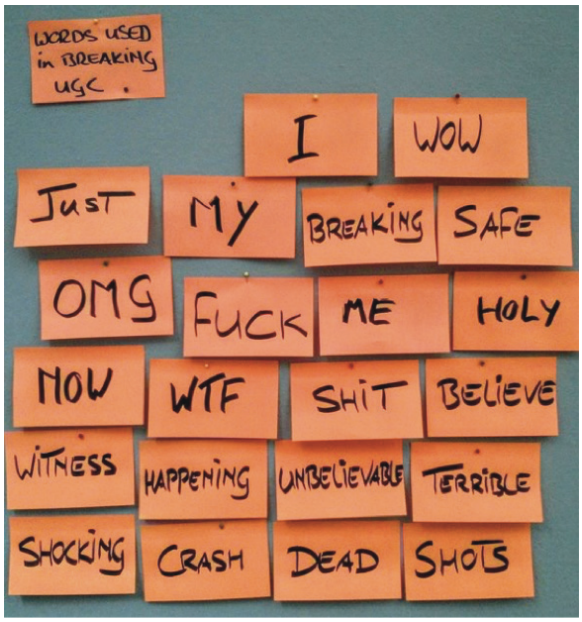


Foto: Ejemplos del tipo de palabras usadas en medios sociales en situaciones de noticias de impacto, incluyendo "I" (yo) y "my" (mi), lo que podría ayudarle a buscar testigos presenciales. Fuente: Deutsche Welle/Reveal Project

¿Puede acotar su búsqueda y filtrar los resultados?
Algunas plataformas de medios sociales permiten buscar por ubicación, dato, 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 monitorizar el contenido de forma selectiva.

¿Ha guardado el contenido que está revisando?
El contenido en línea puede desaparecer muy rápidamente, eliminado por quien lo subió o por la red social que lo aloja. Haga capturas de los mensajes o descargue las imágenes. Para los vídeos, hay herramientas como ***VideoVault***.

¿Puede verificar la información?
Los mensajes en medios sociales han de ser examinados cuidadosamente por precisión. La tentación de usar contenido visual ampliamente compartido sin criterio puede ser más alta que con unas declaraciones de testigos presenciales, pero se debe aplicar el mismo criterio de verificación.

¿Tiene otras fuentes de información para corroboración?
No confíe en un único mensaje de medios sociales cuando sea probable que otros mensajes, vídeos y fotos en línea referencien el mismo incidente. Combinar distintas piezas de información e incluir testimonios de testigos presenciales y reportajes de noticias, le ayudará a construir un caso mucho más fuerte.

¿Hay riesgos de privacidad o preocupaciones éticas?
Como con cualquier fuente, considere los riesgos potenciales para los individuos si comparte o hace públicas sus palabras o imágenes. Además, pregúntese a si mismo si puede 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, o DNH) es un marco útil a tener en cuenta en el contexto de la transformación de conflictos (armados o de otra índole). Este principio requiere plantear cuestiones acerca de si las intervenciones contribuyen a la **unificación** o a **división** adicional.

Compartir imágenes o vídeos con fuerte carga de 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 cuestiones éticas sobre compartir contenido de medios sociales, y resalta la importancia máxima de la verificación y la presentación ponderada de datos con miras a finalizar la violencia en lugar de perpetuarla.

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.*

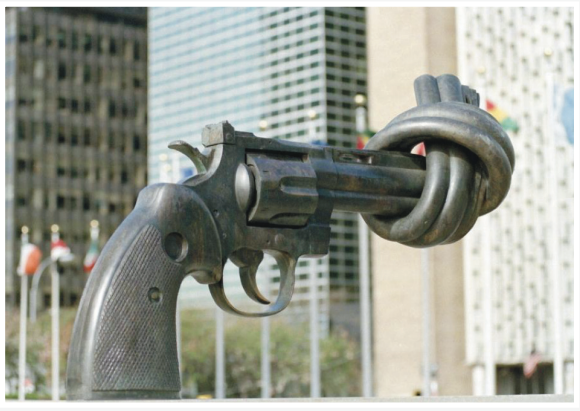


Foto: "***No-Violencia***", UN Photo/ Michos Tzovaras (CC-BY-NC-ND 2.0)

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

Atribución errónea

Este es de largo el desafío más dominante 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 se puede hacer con la imagen de ejemplo de un vídeo. (Vea el capítulo de verificación de esta guía).

Escenificación

Una situación o 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

Sea consciente de la facilidad cada vez mayor con la que el contenido, especialmente las imágenes, puede ser manipulado, recortando, borrando detalles o fundiendo imágenes, para representar los eventos distorsionados.

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 mofas 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 ***acusó a un antiguo combatiente en Siria*** de 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 quiere que sus datos deriven en acusaciones criminales, necesita asegurarse 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.

Considere además la cadena de custodia. Para que sean aceptadas para una acusación criminal, la mayoría de tribunales necesitan conocer cada individuo que manejó el contenido, comenzando por el creador original y terminando por la acusación en el tribunal. La cadena de custodia debe mostrar exactamente quién poseyó el contenido para salvaguardarlo de la manipulación de la evidencia, cuándo, y durante cuánto tiempo. Cuanto más cerca esté 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 trabaje imparcialmente y minimice cualquier posible alteración de los datos. Un abogado defensor podría argumentar que los datos han sido corrompidos, sesgados, o que trasladan motivaciones inapropiadas. Necesitará llevar a cabo al menos algún análisis para conseguir que la documentación sea indexada para búsquedas y hacerla comprensible, pero trate de mantener al mínimo el posible impacto de este análisis.

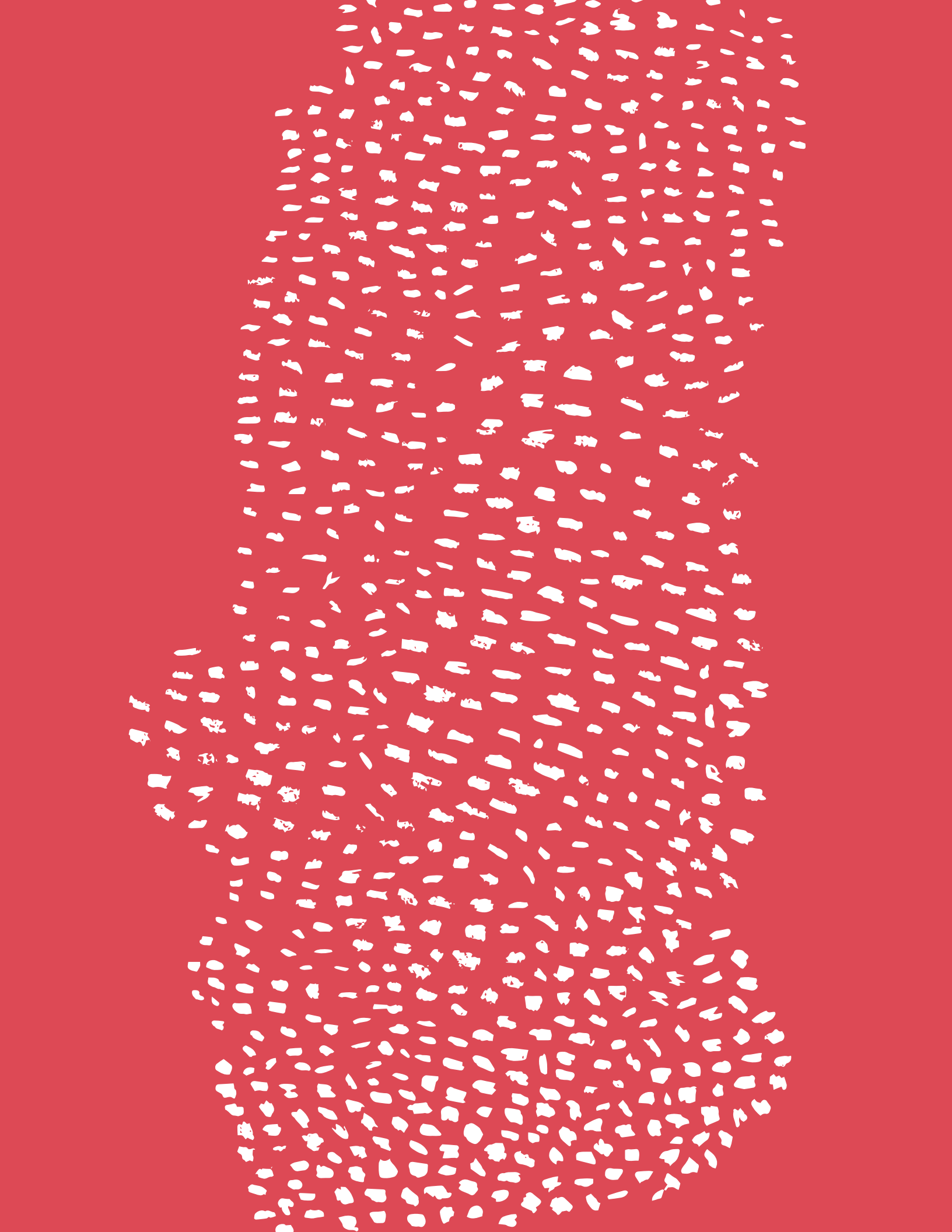
Riesgos de tomar parte en los tribunales
Al tomar parte en los procesos de justicia, las organizaciones de derechos humanos se arriesgan a recibir citaciones judiciales para divulgar evidencias confidenciales, como nombres y fechas, en tribuna abierta, debido al procedimiento previo al enjuiciamiento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

Si está trabajando con la acusación, intente establecer un sistema de protección de testigos. Muchos procedimientos judiciales son públicos, y todas sus precauciones podrían venirse abajo instantáneamente si el testigo declara y su nombre e información personal se hacen públicos. Evite personarse en tribunales que no protegen a los testigos, para que los suyos no sean dañados a resultas 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 ayudarle 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 la no recaída en la situación previa.



Técnicas prácticas

ESTADÍSTICAS ABIERTAS DEL GOBIERNO

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 implicación 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. Lea más 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.	El sesgo en la selección puede llevar a que la muestra sondeada no sea representativa 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 de la monitorización 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 sesgos en la forma de recopilar los datos (ej., en la forma de elaborar las preguntas del sondeo, o de muestrear 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 guiadas, y por tanto predisponen la respuesta.
- **¿Cuál es el tamaño de la muestra?** Puede ser demasiado corta para ser representativa.
- **¿Cada cuánto se recogen los datos?** Los datos pueden estar desfasados.
- **¿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.

Analizar estadísticas desde una perspectiva de derechos humanos

Cuando los datos del gobierno se combinan con, y se analizan contra los estándares y principios de los derechos humanos, pueden ser útiles para evidenciar violaciones de derechos económicos sociales y culturales. Al mirar estadísticas del gobierno es útil, por tanto, preguntarse: ¿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 entre los peores y los más inequitativos. 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 se relacionó 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 yendo a la capital que a Quiché, la región más pobre.

El bajo gasto 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 fiscales e incentivos.

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: ***Escena de calle, 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 deliberadamente, 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 periodos 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 alfabetización en 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 ingresos, personales, ventas de bienes y servicios, beneficios corporativos, etc.).
- Impuestos pagados por distintos grupos en porcentaje del total de 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), pero los núcleos familiares pobres en asentamientos informales confían en el saneamiento in-situ (ej. letrinas en 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 estándares internacionales de derechos humanos como la consecución progresiva de reformas, la no discriminación, y el máximo aprovechamiento de los recursos disponibles, pueden ayudar a responder esta cuestión: ***http://www.internationalbudget.org/publications/escrarticle2/***.

En profundidad

¿Qué es el presupuestado de género?

El presupuestado de género es un tipo concreto de análisis presupuestario usado para evaluar el impacto del gasto del gobierno sobre 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 presupuestado de género es una forma nueva y en evolución de visualizar y afrontar los efectos discriminatorios de decisiones futuras. Hay recursos 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, monitorizar 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 su gobierno, visite 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 su región y 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.

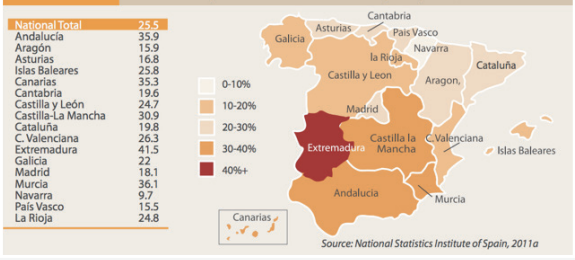
España aprobó el mayor recorte presupuestario de su historia democrática en mayo de 2012, un total de 27,3 millardos de €. El motivo era reducir el déficit público. Sin embargo, expertos advirtieron de que estos recortes se hicieron a costa de la accesibilidad y sostenibilidad de los servicios sociales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

De acuerdo a una percepción equivocada, 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 sumergida, que causó una pérdida significativa de recaudación. El sindicato de supervisores fiscales calculó que si España pusiera el tamaño de su economía sumergida en línea con los estándares de la Unión Europea, sería capaz de generar 38 millardos de €, excediendo el total de recortes presupuestarios para 2012.

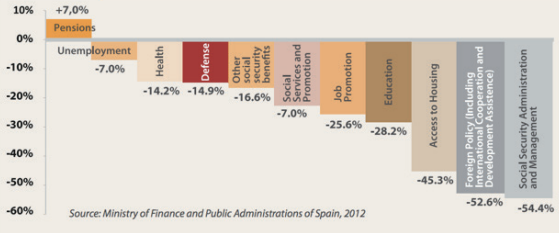
Los investigadores concluyeron que centrándose casi exclusivamente en los recortes de gasto público, las personas estaban siendo privadas de sus derechos sociales fundamentales. Y sin considerar alternativas para reducir el déficit, España no cumple con sus obligaciones bajo el Pacto Internacional de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

FIGURE 11 Percentage of the Population at Risk of Poverty or Social Exclusion by Autonomous Community in Spain (2010)



Source: National Statistics Institute of Spain, 2011a

FIGURE 14 National Budget Cuts to Social and Other Sectors: Percent Change from 2010-2012



Source: Ministry of Finance and Public Administrations of Spain, 2012

FIGURE 15 Annual Expenditure on Social Protection, Health and Education per Capita in the EU-15 (latest figures available)

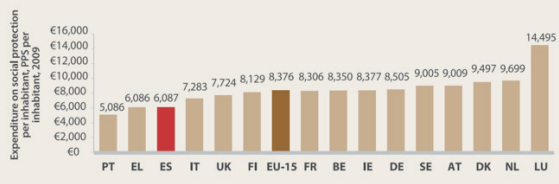
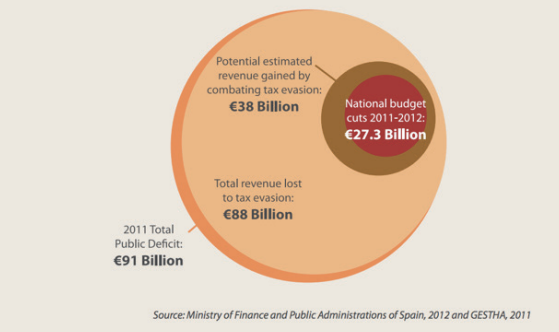


FIGURE 19 Tax Evasion vs. Budget Cuts in Spain (2012)



Source: Ministry of Finance and Public Administrations of Spain, 2012 and GESTHA, 2011

HOY AQUÍ, PERDIDO MAÑANA: PRESERVAR VÍDEOS Y FOTOS EN LÍNEA

Imagine que ha 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 esté trabajando, así que guarda 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 porqué 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 plataforma por cualquiera de 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.

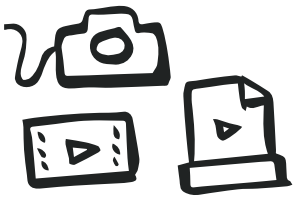
Preservar contenido en línea como fotos y vídeos, incluyendo sus metadatos, asegurará que podrá acceder a ellos en el futuro y ayudará a mantener la integridad de la investigación, le permitirá catalogar los datos y establecerá una cadena de custodia para su uso en ámbito legal.

Cómo descargarlos

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 de navegador 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 publicador o creador original del 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 centrada sobre el trabajo en derechos humanos, considere usar una VPN al buscar y descargar materiales sensibles.



En profundidad

Pasos básicos de preservación

1. **Decida qué contenido es el más relevante** para su proyecto y qué ficheros quiere conservar. Trate de descargar el fichero más grande posible y guarde los ficheros en su formato original.
2. **Use un modo consistente de organizar sus fotos y vídeos.** Por ejemplo, nombre una carpeta en función del año, mes y día: 2016-03-16. Dentro de la carpeta, nombre los ficheros de forma que sean listados en orden cronológico: ***00001.AVI***, ***00002.AVI***, etc.
3. **Use un fichero de texto aparte para documentar los metadatos.** Si el metraje es violento o muy gráfico, incluya una nota clara sobre esto para prevenir al público. El documento de texto debe estar guardado junto al fichero de vídeo o imagen. Si está recopilando grandes volúmenes de contenidos, considere crear un catálogo.
4. **Guárdelo 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 realice una copia de seguridad en dos unidades o dispositivos separados que sean conservados en distintas ubicaciones. Considere usar un almacenamiento en la nube centrado explícitamente en almacenamiento seguro de datos, como SpiderOak o TeamDrive.
5. **Compruebe sus ficheros y unidades periódicamente.**

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

Capturar streams de vídeo

Los streams en directo pueden proporcionar una excelente evidencia inalterada en tanto sean archivados de alguna forma durante la emisión. Muchas plataformas archivan automáticamente los streams en vivo. Si no, tiene que anticiparse a la necesidad y tener software instalado en su 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.

ORGANIZAR SU 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 desarrolladores identificar rápidamente los ficheros correctos, y ahorrar un tiempo valioso.

¿Qué va en la colección?

Antes de elaborar un catálogo, es útil identificar los resultados, objetivos y usos deseados del catálogo. Esto ayudará a asegurar que el contenido que recopila y cataloga es relevante.

- **¿Por qué existe el catálogo? ¿A qué objetivos sirve este?**
  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 aceptará? ¿Qué no aceptará?
  - ¿Cómo se le transmitirán a usted los datos?
  - ¿Qué fuentes o formatos recogerá? Testigos presenciales, noticias/ medios, streams en vivo, etc.
- **¿Qué riesgos está dispuesto a tomar?** ¿Grabaciones que podrían ponerle a usted y a otros en riesgo, o ser citado judicialmente?
- **¿Precisan sus datos ser interoperables con los sistemas de alguien más?**

Acceso: Identifique a sus usuarios y contribuidores

Comprender quién usará y contribuirá al catálogo le ayuda a tomar decisiones sobre accesos y permisos. Al considerar asuntos de seguridad, identifique a qué amenazas puede enfrentarse si el catálogo se hace público o se almacena en una plataforma no segura.

- **¿Quiénes son los usuarios?** Determine 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 alfabetización tecnológica tienen? ¿Qué idiomas hablan? ¿Qué formatos de fichero usan?

Establecer una dinámica de trabajo y seleccionar una plataforma

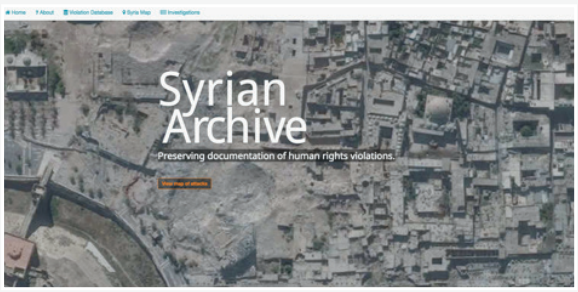
- **¿Cuál es su dinámica de trabajo para asimilar, verificar y catalogar contenido?** Ej., informes de testigos, formulario en línea, hoja de cálculo, formulario impreso, etc.
- **¿Qué plataformas satisfacen los requisitos de su estructura de datos?**
- **¿Cuáles son sus restricciones tecnológicas?** Ej., sin Internet, fondos limitados, sin expertos técnicos, etc.
- **¿Es compatible la plataforma con su entorno de computación?**
- **¿Qué lenguajes necesita 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 sus datos?** Piense en la seguridad mientras los datos se transmiten, 'información en movimiento', y mientras están almacenados, 'información en reposo'.
- **¿Cómo compartirá la información con su 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 ficheros, crearon un catálogo extensivo para capturar los metadatos de cada fichero.

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.

Estructurar su catálogo

La colaboración con los usuarios finales ayuda a identificar la mejor estructura para su 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?** Considere 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?**
- **¿Necesita preservar y catalogar la cadena de custodia porque su documentación podría ser usada para acusaciones criminales en el futuro?**
- **¿Qué información necesita que sea retenida por motivos de seguridad?**

Retención: Planificar una vida de almacenamiento realista para su catálogo

Conocer el periodo esperado de uso para su catálogo le permite planificar mejor su proyecto, asignar recursos y definir el éxito del proyecto.

- **¿Durante cuánto mantendrá el catálogo?** ¿Conservará ciertos tipos de contenido más tiempo que otros?
- **¿Qué ocurre con el catálogo?** Decida sobre un plan de sucesión: eliminación responsable, entrega de los datos, etc.
- **¿Es realista su política de retención?** Ej., ¿puede permitirse seguir con lo que está planificando durante tanto tiempo como está planeando? ¿Tendrá personal dedicado para mantener, actualizar y monitorizar el contenido, para toda la vida de la colección?

Ejemplos de plataformas

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

Caso de estudio

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

En 2012, ***WITNESS*** colaboró con activistas, abogados e investigadores, para amplificar y documentar casos de deshaucios 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 deshaucios forzados relacionados con la construcción 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 deshaucios.

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

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

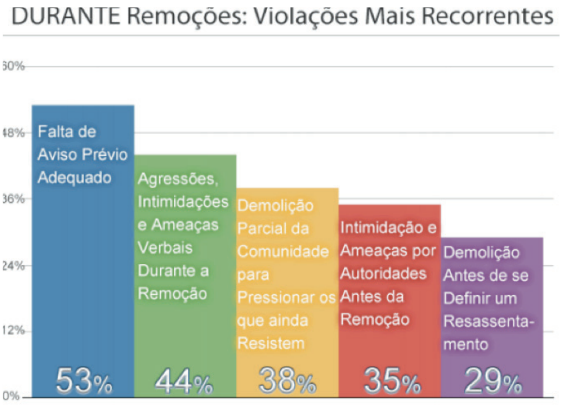


Foto: "*Luchando por la justicia en Brasil*" Protesta anti-deshaucio en Maua, Brasil 2013, por CAFOD Photo Library en Flickr, CC-BY-NC-ND 2.0 *https://www.youtube.com/watch?v=2eAIKhFj0m4*

TAL COMO SE VIO DESDE ARRIBA: 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 quiere lanzar su propio dron hay recursos útiles disponibles para ***iniciarse, desplegarse***, y comprender las ***regulaciones*** nacionales y locales (asegúrese de conocer las reglas o se podría arriesgar a ser multado, ser confiscado su equipamiento, ¡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.

A menudo 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 de satélite proporcionadas por Amnistía Internacional y Human Rights Watch. Es un poderoso ejemplo de cómo las imágenes de satélite puede hacer avanzar la investigación y la defensa de los derechos humanos.

Las imágenes de satélite 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 de satélite en su labor diaria en derechos humanos.

Beneficios de las imágenes de satélite

- **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 de satélite 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 de satélite pueden suministrar potentes visuales, y en movimiento, 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 los medios sociales, la fuente original de una imagen de satélite 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 de satélite captan más información que el ojo humano, como luz infrarroja o ultravioleta, que se puede usar para resaltar la vegetación y medir su salud. 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.

Límites de la imagen de satélite

- **Interpretación**
  El análisis de imagen puede ser susceptible a la interpretación errónea, especialmente si es realizada por analistas o investigadores no instruidos en análisis de imágenes de satélite. 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 monitorizan 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 cubierta nubosa puede entorpecer fuertemente la usabilidad de las imágenes.
- **Áreas problemáticas**
  Las imágenes de satélite 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 imagen de satélite.

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 el deslizador de imágenes yuxtapuestas en el menú "Imágenes históricas" de 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 de satélite en informes en línea, se puede crear un deslizador de imágenes yuxtapuestas simple que permita al lector explorar cambios temporales por si mismo. Una herramienta fácil y gratuita para incrustar estos deslizadores es ***Juxtapose***.

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

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

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

Fuentes de imágenes de satélite con resolución inferior al metro

› **Google Earth**: Puede ser una herramienta altamente útil como fuente de imágenes de satélite gratuitas. Sin embargo, a veces tiene baja resolución en algunas zonas como resultado de la presión política.

› **TerraServer**: Un proveedor de imágenes de satélite de DigitalGlobe. Se puede usar de forma gratuita en apoyo de la investigación básica, y a menudo proporciona más imágenes 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 (apenas el tamaño del sujeto/objeto más pequeño que se puede identificar en una imagen). El tamaño mínimo a encargar para la compra de imágenes es de 25 Km^2. 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 monitorización constante desde el espacio. Las compañías antes mencionadas sólo pueden proporcionar capturas de ciertas áreas del planeta. Permanezca atento al ***vídeo de satélite***, que tendrá grandes implicaciones para la investigación en derechos humanos. Una pega 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 seguridad física y la certidumbre en el contexto de los 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 directamente una senda dañina.

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 la digital 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 nombre, caras, y/o la información de un gran número de víctimas u otros individuos vulnerables será comprometida. Su obligación es dar los pasos para protegerse a usted mismo y a otros de daños adicionales.

La gente concernida por los datos entra 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 la gente no se da cuenta de que un vídeo que están publicando en línea contiene información sensible. Si usted, como profesional en derechos humanos, decide usar un vídeo para una campaña, la fuente y el creador pueden ser señalados como objetivo por estar afiliados con su grupo, incluso si nunca supieron de ustedes.

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

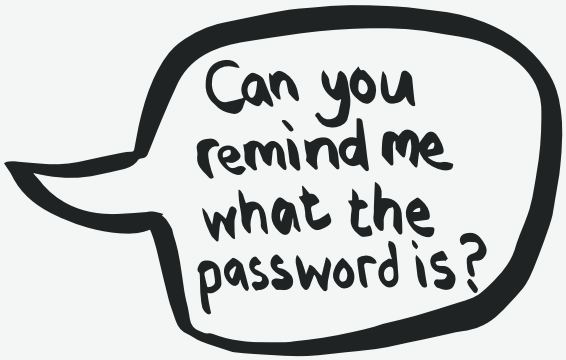
En el caso de que haga públicos los datos, o que haya una brecha de seguridad, la fuente y los individuos retratados se exponen a un mayor riesgo de daño físico, incluso si su información ya se había publicado en línea. Peor aún, puede ser difícil informar a cualquiera de estos individuos de la elevación del 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*** para fijar el objetivo en 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 sucumbido 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.



Para evitar ser atacado mediante técnicas de ingeniería social, sea vigilante 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 del poseedor de la cuenta. Evite también compartir información sensible a través de medios sociales o correo electrónico, sin tener implementadas medidas de seguridad adicionales.

DATOS RESPONSABLES

Datos responsables es:
El deber de asegurar el derecho de las personas al consentimiento, privacidad, seguridad y propiedad en torno a los procesos de la información de recopilación, análisis, almacenamiento, presentación y reutilización de los datos, mientras se respetan los valores de transparencia y aperturismo
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 apúntese 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 afianzar la seguridad y bienestar de la gente con la que trabaja. La plétora de asuntos éticos que podrían surgir, se podrían tomar en consideración como **desafíos de datos responsables**. No hay una política establecida que vaya a funcionar para todas las situaciones, pero le animamos a que reflexione sobre los siguientes asuntos dentro del contexto de usted:

- **Consentimiento informado**
  Especialmente dentro del ámbito de las violaciones de derechos humanos, obtener consentimiento informado puede suponer mucho más de lo que pueda pensar en un principio. Asegúrese 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, intente recopilar la cantidad mínima de datos necesarios para su propósito específico.
- **Datos personales**
  Siempre que sea posible, si tiene nombres, fechas de nacimiento u otra información con capacidad de identificación personal, trate de desvincularla o borre lo que no necesite.
- **Datos sensibles**
  Sea consciente de dónde se almacenan los datos sensibles sobre raza, etnicidad u orientación sexual, si están en sus servidores o en un país extranjero (ej., al usar un servicio de Google) por si acaso pudieran dejar expuestos al riesgo a los individuos.
- **Sesgo implícito**
  Los datos reunidos de otras fuentes pueden ocultar sesgos. Piense detenidamente acerca de las decisiones humanas que se tomaron durante el análisis.

Información proveniente de medios 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. Tiene 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.

Proteger la identidad de las personas en medios sociales

Los mensajes en medios 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 es usted personalmente quien publica estos datos, como si lo hace en nombre de una organización que desea volver a publicarlos, debe 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 está grabando, como cuando carga algo desde su biblioteca. Recientemente YouTube también ha añadido una ***característica de difuminado*** que le permite oscurecer caras cuando carga un vídeo.

¿SON SEGURAS SUS HERRAMIENTAS DIGITALES?

Cuando se trata de hacer copias de seguridad, almacenamiento de ficheros seguro, 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 aparcados (un fichero guardado en su disco duro).

Damos estos pasos porque en la recopilación, conservación y compartición 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, pregúntese a si mismo...

1. **¿Qué significa "seguro" en realidad?**
Decir que un software es "seguro" puede significar distintas cosas. Lea 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 las computadoras de usted y los servidores de ellos—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 los servicios. Es importante comprender esta distinción, y considerar si es relevante para su proyecto mantener ocultos los datos de los proveedores de servicios.

2. **¿Ha sido auditado el software de forma independiente?**
No se limite 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 use software que haya sido auditado por alguien en quien confíe. Preferiblemente el software debe ser de "código abierto", y este estar disponible para su escrutinio público. E incluso entonces, no puede estar seguro de que unos resultados de auditoría limpios no se hayan dejado vulnerabilidades. Mantenga siempre un saludable escepticismo.

3. **¿Quién tiene en su poder los datos — y por cuánto tiempo?**
Cuando use un servicio en línea para comunicarse, crear o archivar información, debe 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 típico que estén sepultadas en las Condiciones de Servicio de una compañía. Cualquiera que sea el servicio que use para archivar o compartir datos sensibles, debe investigar sus políticas sobre compartición de datos con otras compañías y gobiernos, y qué es lo que puede esperar que ocurra con los datos si borra su cuenta o la compañía es vendida o cierra.

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

5. **¿Le dejará expuesto su uso del software o servicio?**
En algunos lugares el uso de cifrado es ilegal. En otros no lo es, pero todavía levanta sospechas de las fuerzas de la ley o de agencias de inteligencia. Esto puede llevarles a monitorizar la actividad de una persona simplemente porque ha comenzado a usar software de cifrado. Es importante comprender su 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 permitirle mantener un perfil bajo y atraer menos atención. Conocer su contexto es esencial para hacer este tipo de valoración.

6. **¿Es práctico para usted adoptar este software o servicio?**
Algunos servicios o software pueden encajar bien en los procesos existentes que está usando para recopilar, almacenar, analizar, y compartir datos. Otros puede que requieran una reconversión importante a los nuevos procesos. 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. **¿Está adoptando esta aplicación por las razones correctas?**
Hay muchas razones por las que podríamos estar interesados en un nuevo servicio o herramienta: Estar atractivamente diseñado, tener un nombre interesante, prometer un servicio novedoso, estar creciendo en popularidad, etc. Revise de forma dura y crítica las razones por las que está considerando adoptar una herramienta y asegúrese de que parecen ser las razones *correctas*, dadas sus necesidades y obligaciones éticas y de seguridad.

Es muy raro que cualquier 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 este aviso, ¿se siente de forma distinta acerca de cualquier herramienta o servicio que haya adoptado recientemente? ¿Sigue siendo la elección correcta para usted?

En profundidad

Anticipo sobre vulnerabilidades.

Algunos desarrolladores publican "modelos de amenaza" y vulnerabilidades conocidas en su sitio web en aras de la transparencia. Para buenos ejemplos, vea la documentación para ***Scramble.io*** (software de correo electrónico seguro) y ***Cryptocat*** (software de chat seguro). Ahora más compañías publican también informes de transparencia que destacan cosas como peticiones oficiales de información de usuarios y notificaciones legales de desmantelamiento. Por ejemplo, vea el ***Twitter's Transparency Report*** (Informe de Transparencia de Twitter). Estos informes son voluntarios y difíciles de verificar, pero todavía 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 monitorizado 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 de amplia confianza de Signal en 2016, que es de código abierto y verificable. 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 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 movilización de recursos, y habilita la preparación para los riesgos inherentes al trabajo en derechos humanos.

La certidumbre está relacionada con la seguridad física, salud, finanzas, discriminación, privacidad, etc. Las amenazas de 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 cualquiera que esté involucrado en su trabajo, es el primer paso en el fomento de un entorno productivo y seguro.

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

- Explore las tendencias políticas, económicas, sociales, tecnológicas, legales y ambientales inherentes a su trabajo.
- Identifique y analice amenazas de seguridad concretas y tome las medidas necesarias para prevenirlas o responder a ellas.
- Identifique a sus aliados y oponentes, sus intereses y su potencial para capacitarle o para actuar en su contra.
- Cartografíe y categorice la información y datos privados, y tome medidas para protegerlos de pérdida o daño.

Amortiguar el trauma secundario 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 visionar 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 de la 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

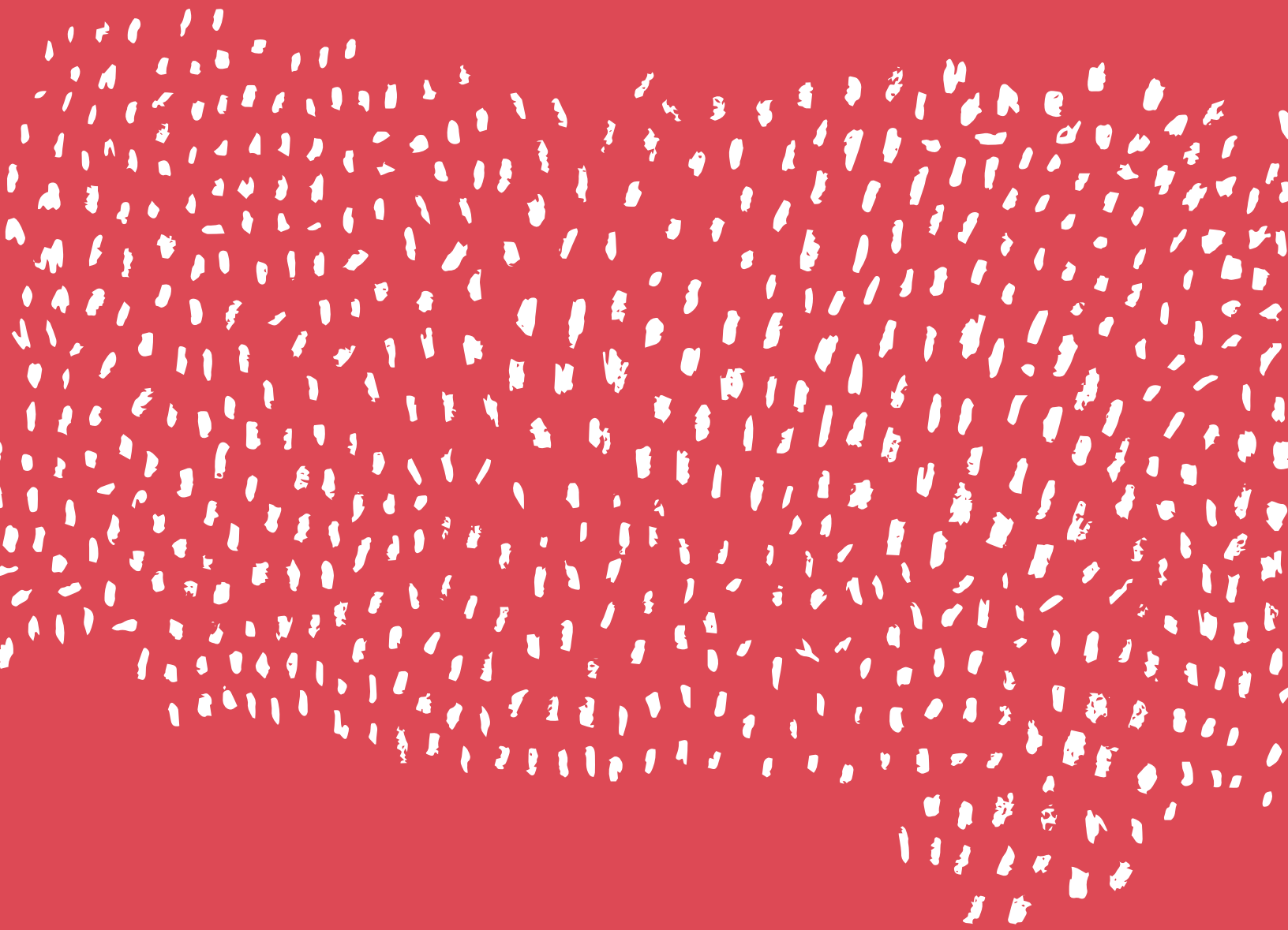
- Dificultad para gestionar sus emociones.
- Dificultad para aceptarse o sentirse bien consigo mismo.
- Dificultad para tomar buenas decisiones.
- Problemas para gestionar límites. Ej. tomar demasiada responsabilidad, tener dificultades para abandonar el trabajo al final de día, tratar de inmiscuirse y controlar las vidas de los demás.
- Problemas con sus relaciones.
- Problemas físicos como dolores y achaques, indisposición, o accidentes.
- Dificultad para sentirse conectado con lo que ocurre alrededor y consigo mismo.
- Pérdida de significación y esperanza.
- Incremento del abuso de sustancias, alcohol en particular.
- Comilonas desmedidas.
- Aislarse a si 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. Marque la frecuencia con la que el personal se expone a contenido traumático.
2. Elimine la exposición repetida innecesaria.
3. Revise los procedimientos de ordenación y etiquetado para reducir el visionado innecesario.
4. Pruebe distintas formas de visionado. Algunos encuentran que concentrarse en ciertos detalles, por ejemplo ropa, y evitar otros (como caras) puede ayudar a crear una distancia emocional.
5. Ajuste el entorno de visionado: reduzca el tamaño de la imagen o vídeo, o ajuste el brillo/resolución de la pantalla.
6. Apague el sonido cuando sea posible.
7. Tómese descansos frecuentes de la pantalla. Mire algo agradable, estire las piernas o dé un paseo.
8. Cuando envíe correos con contenido gráfico, añada una advertencia del contenido en la línea del asunto.
9. Etiquete claramente todos los ficheros al archivarlos, para que nadie se exponga accidentalmente a contenido explícito.
10. Elabore su propio plan de auto-atención. 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. Establezca 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 es profesionalmente tratable. Si cree que usted o un colega pueden estar sufriendo de TEPT, busque ayuda profesional de inmediato.



A dónde ir desde aquí

CÓMO ENCUADRAR SU INVESTIGACIÓN

Antes de entrar en análisis, piense con detenimiento sobre lo que representan sus datos y qué conclusiones válidas puede extraer de ellos. Esta sección le ayuda a establecer la representatividad de un conjunto de datos y precisar dudas para evitar conclusiones inapropiadas o incorrectas.

Establecer qué tipo de muestra son sus datos

Hay tres tipos de muestras. El tipo de muestra que tiene 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.

Determinar qué conclusiones puede extraer

El proceso de aprendizaje y extracción de 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 tiene.

Hacer inferencias de muestras completas

Las muestras completas son especiales porque son idénticas a la población, así que lo que quiera que aprenda acerca de la muestra, también lo aprende sobre la población.

Hacer 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 estadística, la población se refiere a todas las unidades de análisis que quiere estudiar.

Ejemplo 1
Quiere conocer a cuántos refugiados que están entrando al país X por barco se les está denegando el acceso a tratamiento sanitario. La población son todos los refugiados que llegaron al país X por barco y les fue denegado el acceso a atención sanitaria.

Ejemplo 2
Está examinando si las industrias de flores comerciales han causado contaminación del agua en una región determinada. Aquí, X son todas las industrias de flores en esa región

Muestras de conveniencia

Las muestras de conveniencia no son representativas de la población: están sesgadas de formas desconocidas. Todas las muestras de conveniencia contienen sesgos de selección. En términos estadísticos, esto significa que no conocemos completamente hasta qué grado nuestra muestra representa bien a la población. No sabemos qué partes de la población no estamos viendo, cómo es de grande la proporción de la muestra dentro de la población, o de qué manera difiere nuestra muestra de la población.

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 puede 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. Asegúrese 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 que conducen a la denegación del acceso a la atención sanitaria.
- Hacer constar dónde y en qué momentos ha identificado estas prácticas. Si ha documentado estas prácticas en varias instalaciones sanitarias por todo el país X y/o repetidamente a lo largo del tiempo, puede 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 haya sido capaz de identificar más de ellas. Para apoyar esta afirmación podría listar las instalaciones que pudo 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 puede 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 conoce cuántos refugiados no fue 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 trata la información de su muestra de conveniencia como lo que es —tan solo las evidencias de violaciones de derechos humanos que pudo documentar— tendrá una base más fuerte para justificar sus denuncias sobre derechos humanos en público.

Documentar su proceso de investigación

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

Preguntas sobre la muestra que su metodología debe tratar de resolver

- **¿Cuál es el foco geográfico de su estudio?**
- **¿Cuál es el foco temporal de su estudio?**
- **¿Cómo midió X?**

a. Fuente de datos principal

i. ¿Dónde y cuándo fue descargada?
ii. ¿Quién fue el creador/proveedor original? ¿Es creíble esta fuente? ¿Cómo verificó estos datos?
iii. ¿Está disponible públicamente?
iv. ¿Organizó 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 trató con la información perdida?
vii. ¿Términos de búsqueda usados, hashtags seguidos? ¿En qué idiomas?

- **¿Qué métodos usó para extraer los resultados de los datos recogidos?**

b. Procesamiento y gestión de los datos

i. ¿Proceso de traducción?, si es aplicable.
ii. ¿Software usado?
iii. ¿Proceso de combinado/vinculado de diferentes fuentes de datos?

c. Análisis de datos

i. ¿Software/lenguajes de programación usados?
ii. ¿Métodos estadísticos empleados?
iii. ¿Procedimiento para tratar con información perdida?
iv. ¿Tipos potenciales de comprobaciones de fortaleza y análisis de sensibilidad?

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

Los investigadores tienen más fácil acceso que nunca antes a los datos. Pero muchos todavía carecen de las destrezas o confianza para trabajar con grandes conjuntos de datos. En el ya ahogado de presupuesto y cargado de trabajo, campo de los derechos humanos, esto pone a los expertos en datos bajo una presión particular mientras luchan por satisfacer las muchas demandas de sus colegas. Cuanto más educado y capacitado esté para realizar su trabajo, más estrés y tiempo se ahorrará a usted mismo y a sus colegas.

Dicho esto, a veces necesita llamar a los expertos. Antes de hacer algo así, prepárese para su conversación considerando las siguientes preguntas:

- **¿Cuál es su meta final?** Ser explícito sobre sus objetivos ayuda al experto a comprender sus requerimientos.
- **¿A qué se parece un buen soporte?** ¿Está buscando asistencia para comprender el sesgo de un conjunto de datos específico?, ¿o soporte para analizar un flujo de datos que es nuevo para usted?, ¿o quizá confirmación de que está en el buen camino?
- **¿Necesita asistencia específica o continua?** Sea realista y solicite asistencia sólo en la medida en que pueda permitírsela.
- **¿Por qué este experto?** ¿Ha trabajado antes

Haga sus deberes

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

Busque ejemplos de proyectos similares que le gusten, y que usen los nuevos tipos de datos de la forma particular que usted desea. Una vez los encuentre, anote la fecha en la que fueron creados, y seleccione cualesquiera elementos que encuentre particularmente inspiradores o que sean particularmente relevantes para su trabajo. Una vez tenga una lista de proyectos, contacte con algunos de los investigadores involucrados en ellos y vea si tienen tiempo para una llamada rápida con usted. Sea realista: aunque un proyecto concreto podría parecer muy simple desde fuera, puede haber implicado más trabajo entre bambalinas de lo que podría percibir.

Permanezca crítico

Aunque se plantee dudas, todavía posee la mayor pericia en su contexto específico. Si alguien trata de decirle que algo *siempre* o *nunca* es correcto, y usted está en desacuerdo, confíe en su instinto.

Especialmente cuando comience a haber dinero de por medio, recoja múltiples opiniones sobre cuál sería la mejor opción para usted. Los proveedores de software, tanto si están motivados por el beneficio o limitados por una orientación hacia sus propios productos, puede que no le proporcionen la mejor recomendación. Considere el más seguro y generalmente menos caro Software Libre y de Código Abierto (FOSS, por sus siglas en inglés) siempre que sea posible.

CONCLUSIÓN

Hay varias organizaciones e individuos que están usando estas técnicas para extender los límites de la documentación de situaciones de derechos humanos, de nuevas y excitantes maneras. Muchos de ellos han sido fuertes fuentes de inspiración para esta guía y para nuestro trabajo colectivo conjunto, facilitándonos en un destello una visión 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 reclamaciones legales en curso consignadas contra estados miembros de la OTAN.

O ***Bellingcat***, una red de periodistas ciudadanos de investigación que usan información públicamente disponible, incluyendo datos de medios sociales, y más generalmente Inteligencia de Código Abierto (OSINT), para investigar violaciones de los derechos humanos y más.

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 estadísticos 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 para 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 más tradicional.

El futuro es nuestro y el momento es ahora

Entre sus destrezas en derechos humanos y la información en esta guía, tiene todo lo que necesita para ponderar el valor de diferentes datos para su trabajo, y comenzar a usarlos.

Las consideraciones, valoraciones, y usos descritos están enraizados en prácticas con las que ya está familiarizado—como aquellas 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 le permiten hacer y cómo, continúa siendo mucho más importante que centrarse en herramientas específicas. Estar al tanto de lo que esas herramientas hacen, los sesgos dentro de los datos que recibe y con los que trabaja, y, sobre todo, ocuparse 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. Sus costes, así como los costes de las tecnologías, 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*** es sede de una comunidad fuerte 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 cribado, hasta el análisis y visualización de los datos. Si quiere apoyo para configurar y usar bases de datos en su proceso de documentación, eche un vistazo en ***Benetech***, o ***HURIDOCS***.

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

Datos de medios sociales

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

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

Citizen Media Research and Verification: An Analytical Framework for Human Rights Practitioners
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://es.witness.org/portfolio_page/normas-eticas-como-utilizar-los-videos-de-testigos-presenciales-para-informar-y-defender-los-derechos-humanos/

Datos presupuestarios para derechos humanos

Center for Economic and Social Rights (2015), Defending Dignity: a manual for national human rights institutions on monitoring economic, social and cultural rights

International Budget Partnership (2010), 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: a guide to budget analysis to advance human rights

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/resources/handbook/***

Hoy aquí, perdido manaña: Preservar 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***

Lumen Database ***https://lumendatabase.org/topics/1*** 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/#lumen***

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 desmantelamiento de YouTube, y cómo desafiarlas ***https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals***

Conozca 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 de satélite ***http://landscape.satsummit.io***

Cree un deslizador de imágenes yuxtapuestas antes/después: seleccione imágenes de satélite y alójelas en línea, por ejemplo, en Flickr. Luego copie y pegue los dos enlaces de Flickr (deben terminar en .jpg) en la herramienta Juxtapose ***https://juxtapose.knightlab.com/#create-new***

Inspírese 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 de satélite 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***

Lista de comprobación de seguridad digital para determinar quién tiene acceso a su contenido ***https://docs.google.com/document/d/17gRphFoh7PlUrmeQNu5ADhNfty-2sEV-CLQN4Ed1hak/edit***

Tal como se ve desde arriba: 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 ***http://twentysix.fibreculturejournal.org/fcj-195-privacy-responsibility-and-human-rights-activism/***

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/pdf/news/protecting_journalism_sources_in_digital_age.pdf***

¿Son seguras sus herramientas digitales?

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

Hacer copias de seguridad de su software *https://securityinabox.org/es/chapter-5*

Almacenamiento seguro de ficheros *https://securityinabox.org/es/chapter-4*

Destruir información *https://securityinabox.org/es/chapter-6*

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/es/module/una-introduccion-al-modelaje-de-amenazas*

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/es*

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

Cómo encuadrar su 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*

Publicaciones escogidas de HRDAG sobre sesgo de selección *https://hrdag.org/publications/big-data-selection-bias-and-the-statistical-patterns-of-mortality-in-conflict/*

Informes que documentan la metodología de la investigación subyacente a modo de una o varias secciones en el informe:

https://hrdag.org/wp-content/uploads/2013/02/Gohdes_Convenience-Samples.pdf

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

Vídeo: WITNESS *https://es.witness.org/*

Métodos estadísticos:
El 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:
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