داتاف

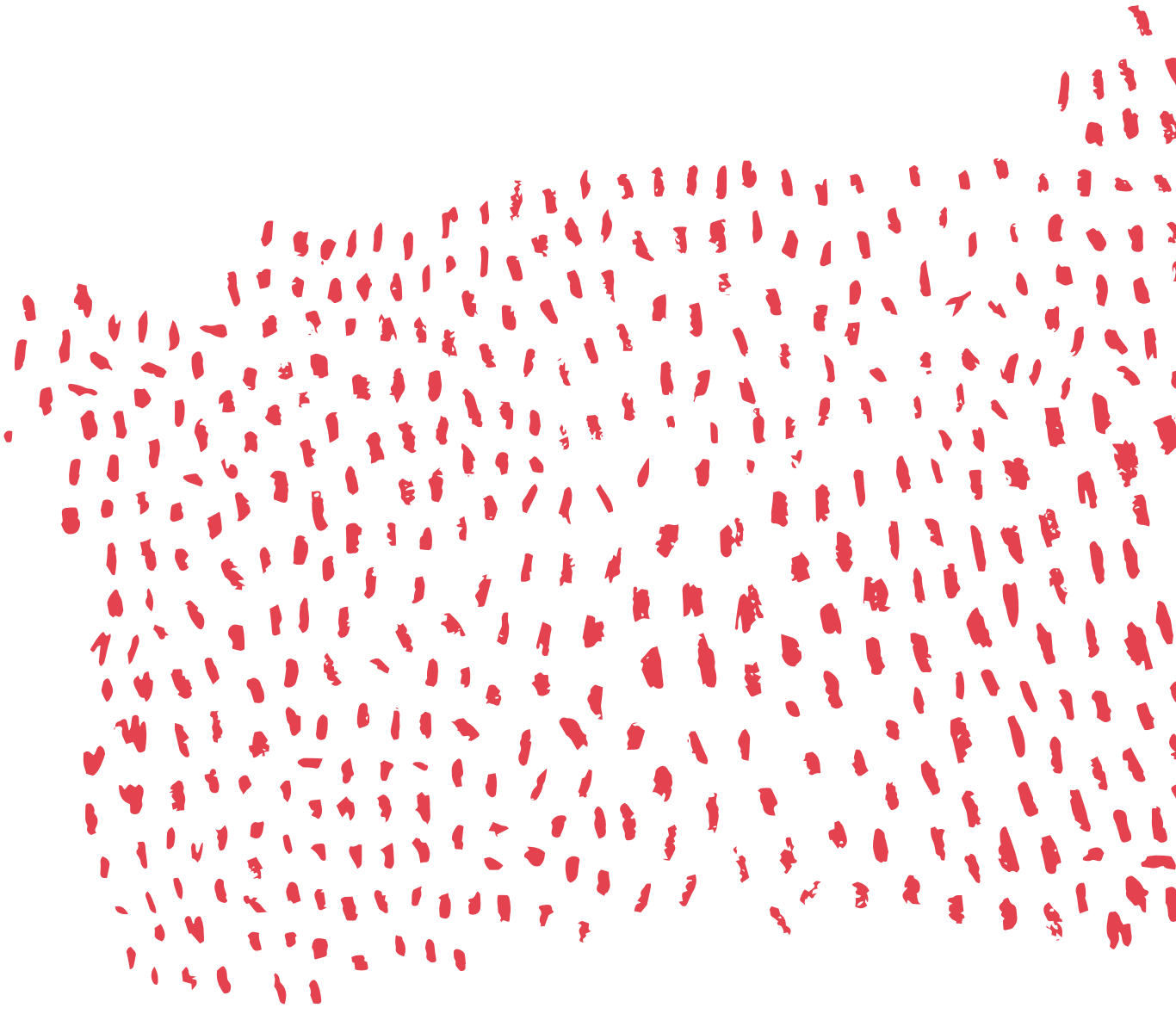
كيف تتصفح البيانات الرقمية لأغراض البحث في مجال حقوق الإنسان

THE ENGINE ROOM

benetech
TECHNOLOGY SERVING HUMANITY

AMNESTY INTERNATIONAL

MEEDAN



Eyewitness Media Hub

University of Essex

GULF CENTER FOR HUMAN RIGHTS

HRDAG

Syria Justice and Accountability Centre

WITNESS SEE IT FILM IT CHANGE IT

المحتويات

البداية

فهم التحقق والتوثيق

تقنيات عمليـة

اعتبارات البيانات المسئولة

إلى أين تذهب بدءًا من هنا؟

المساهمون

نتوجه بالشكر للتالية أسماؤهم من المساهمين في ورشة الكتابة:

- Allison Corkery, Center for Economic and Social Rights
- Sam Dubberley, Eyewitness Media Hub and Human Rights and Big Data Project, University of Essex
- Scott Edwards, Amnesty International
- Lisa Gutermuth
- Danna Ingleton, Amnesty International
- Christoph Koettl, Amnesty International
- Jule Krüger, Human Rights Data Analysis Group (HRDAG)
- Chris Michael, Collaborations for Change
- Ella McPherson, Department of Sociology and the Centre of Governance and Human Rights, University of 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

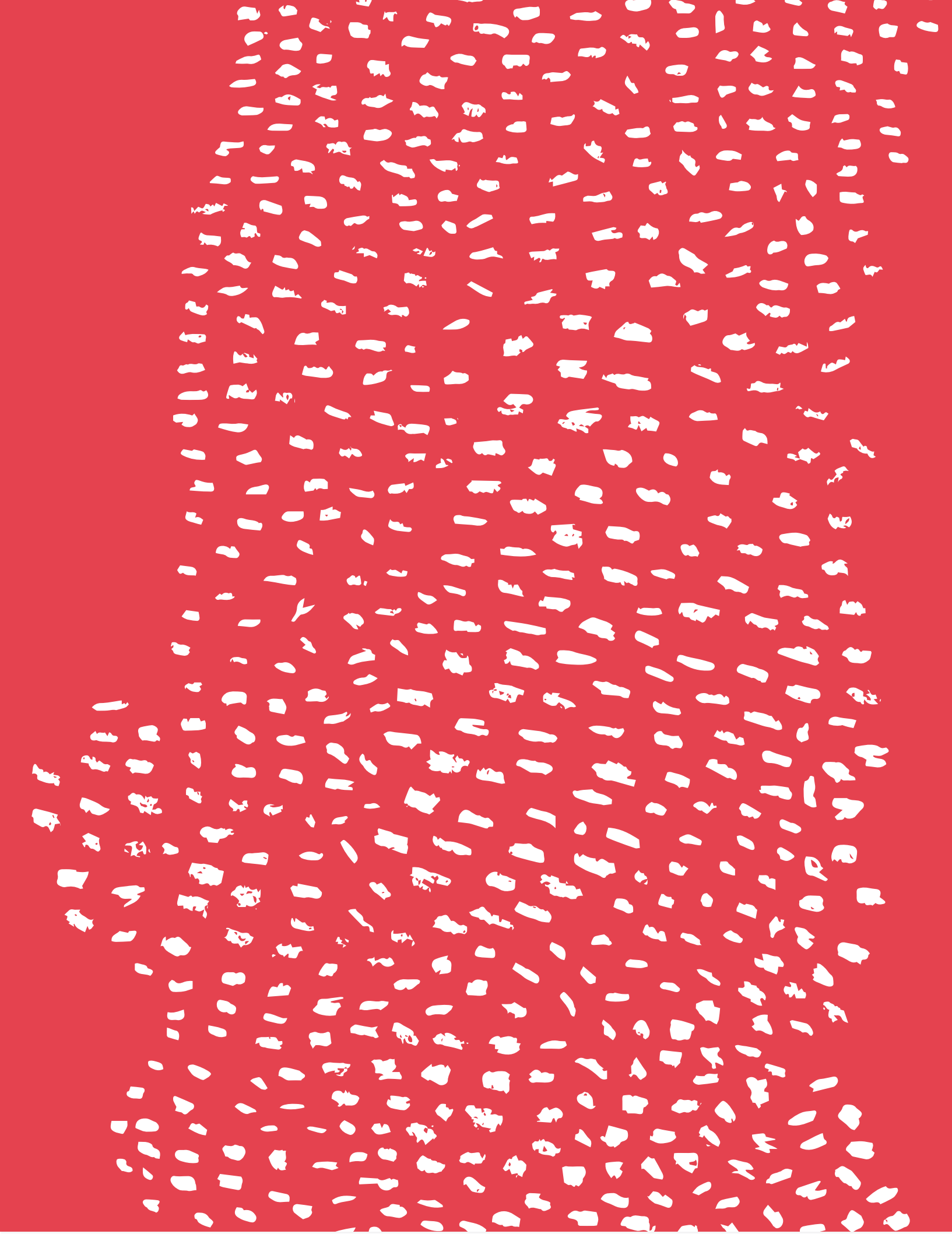
كما نتوجه بالشكر للتالية أسماؤهم ممن أسهموا في المشروع بوصفهم مراجعين لنص الدليل أو مساهمين في الدعوة المجتمعية أو أطراف في المقابلات في مراحل المشروع المبكرة.

- Kristin Antin, HURIDOCS
- Jay Aronson, Center for Human Rights Science, Carnegie Mellon
- Patrick Ball, HRDAG
- Alexis Bautista, Migrant Forum in Asia
- Anh Bui, Benetech
- Neil Blazevic, East and Horn of Africa Human Rights Defenders Project
- Laura Carter, Amnesty Kristy Crabtree, International Rescue Committee
- Elsa Marie da Silva, SafeCity
- Priti Darooka, Programme on Women's Economic, Social and Cultural Rights
- Jessica Dheere, SMEX
- Nicola Diday, swisspeace
- Tarek Dobo, Syrian Justice and Accountability Center
- John Emerson, NYU Center for Human Rights and Global Justice
- Wael Eskandar
- Emmanuel Freudenthal
- Mahbul Haque, Bangladesh Centre for Human Rights and Development
- Morgan Hargrave, WITNESS
- Theresa Harris, AAAS
- Shevy Korzen, The Public Knowledge Workshop
- Tom Longley
- Milena Marin, Amnesty International
- Beatrice Martini, Aspiration
- Ruth Miller
- Tawanda Mugari, Digital Society of Zimbabwe
- Yvonne Ng, WITNESS
- Dan O'Clunaigh

- Ted Perlmutter, Institute for the Study of Human Rights at Columbia University
- Robin Pierro, European Inter-University Centre for Human Rights and Democratization
- Enrique Piraces, RightsLab
- Vanya Rakesh, CIS India
- Vijay Rao, 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

النسخة العربية ترجمت بواسطة ميدان www.meedan.com

فن الغلاف: Lynne Stuart.
تصميم الجرافيك: Fedrico Pinci.
نُشر لأول مرة في يونيو / حزيران ٢٠١٦



البداية

مقدمة

بدايةً من مقاطع فيديو انتهاكات حقوق الإنسان الموجودة على الإنترنت، ومرورًا بصور الأقمار الصناعية للتدهور البيئي، ووصولًا إلى روايات شهود العِيان المنشورة على وسائل التواصل الاجتماعي، أصبحنا قادرين على الوصول إلى بيانات مهمة بشكل غير مسبوق. عند استخدام هذه البيانات بصورة مسئولة، يمكن لها أن تساعد العاملين في مجال حقوق الإنسان في المحاكم، وعند العمل مع الحكومات والصحفيين، وفي التوثيق لأغراض التأريخ.

كما أن تكلفة الحصول على البيانات الرقمية ونشرها وتخزينها تزداد تيسيرًا يومًا بعد يوم؛ كلما استمرت التكاليف في الانخفاض وأنشئت منصات جديدة، زادت فرص تسخير مصادر البيانات تلك للعمل في مجال حقوق الإنسان.

ولكن إدماج عمليتَي جمع البيانات وإدارتها في العمل اليومي الخاص ببحث وتوثيق حقوق الإنسان قد يمثل تحديًا، بل وعائقًا للأفراد والمنظمات. صُمم هذا الدليل ليساعدك على تصفح أشكال البيانات الجديدة وإدماجها في عملك في مجال حقوق الإنسان.

وهو نتاج التعاون بين منظمة العفو الدولية Amnesty International وشركة Benetech (بينيتك) ومنظمة The Engine Room (ذا إنجين روم) الذي بدأ في أواخر عام ٢٠١٥، والذي أسفر في مايو/ أيار ٢٠١٦ عن ورشة عمل مكثفة امتدت على مدار أربعة أيام، صممها ويسرها كريس مايكل من Collaborations for Change (كولابوريشنز فور تشينج). أجرينا سلسلة من المقابلات والمشاورات المجتمعية والاستقصاءات لفهم ما إذا كان هناك دمج للبيانات الرقمية في العمل الخاص بحقوق الإنسان. في الغالبية العظمى من الحالات، وجدنا أن ذلك لا يحدث. لماذا؟

بشكل أساسي، بدا الأمر وكأن باحثي حقوق الإنسان قد بوغتوا بالاحتمالات الجديدة. في مواجهة محدودية الموارد، وبينما لا يعلمون من أين يبدءون أو ما إذا كان الأمر يستحق العناء من الأصل، امتنع معظم من تحدثنا إليهم عن مجرد محاولة تقوية عملهم بالبيانات الرقمية.

ولدعم الجميع في مجال حقوق الإنسان نحو الإبحار في خضم هذه البيئة المعقدة، عملنا مع كريس مايكل من Collaborations for Change (كولابوريشنز فور تشينج) لترتيب اجتماع ١٦ باحثًا وخبيرًا فنيًّا في قلعة خارج العاصمة الألمانيــة برلين في مايو/ أيــار ٢٠١٦. على مدار أربعة أيام من التفكير والكتابة المكثفَين، تعرفنا بصورة جماعية على فجوات المحتــوى والموضوعات الواجب تغطيتها، وقمنا بصياغة هذا الدليل.

هذا الدليل لك

نحن نفترض أنك تعرف كيفية القيام بالبحث في مجال حقوق الإنسان، ولكنك ترغب في توسيع دائرة معرفتك بشأن كيفية استخدام البيانات الرقمية ووسائل الإعلام الإلكترونية لأغراض التوثيق.

إليك مقدمة عامة ستضعك على الطريق الصحيح نحو طرح أسئلتك الخاصة والبحث عن حلولك المتفردة. نحن نسعى نحو قدح زناد قريحتك النقدية بدلًا من توجيهك لاستخدام برمجيات أو أجهزة أو منصات بعينها، بما أن كل هذه الوسائل تتغير وتتطور باستمرار.

وقد قمنا بعملية بحث دقيق للموارد وجمعنا مواد إضافية للقراءة فيما يتعلق بالمسائل التي يعالجها هذا التقرير، يمكنك أن تجدها على شبكة الإنترنت على **https://engn.it/datnav**

كما أننا نتصور أنك باحث في مجال حقوق الإنسان، أو صحفي، أو طالب، أو صانع سياسات أو شخص خيِّر يريد أن:

- يعزز من أساليب البحث والتوثيق التقليدية (المقابلات والاستقصاءات وجداول البيانات) عن طريق تعلم كيفية دمج البيانات الرقمية.
- يبني معرفة وخبرة استباقًا لأي حادث طارئ؛ وذلك من أجل تجنب الجمع الرجعي للبيانات بينما يكون الحدث أو الانتهاك في أوجه.
- يفهم الفرص التي تقدمها البيانات الرقمية وكذا حدودها ومخاطرها، بالإضافة إلى متى وكيف يبحث عن نصيحة ذوي الخبرة للمساعدة في تحقيق أهدافه.
- يتغلب على الخوف من البيانات والتكنولوجيا الرقمية التي يستخدمها نظراؤه بالفعل على نطاق موسع. باستخدام الأدوات الأفضل، تيقن من أنك ستكون أكثر كفاءة.

الإمكانيات الجديدة التي تتيحها البيانات الرقمية

بعض أشكال البيانات الرقمية التي يناقشها هذا الدليل:

- الصور ومقاطع الفيديو والميتاداتا الخاصة بها
- صور الأقمار الصناعية والمعلومات الجغرافية المكانية
- محركات البحث ووسائل التواصل الاجتماعي والآراء على الإنترنت
- إحصاءات الحكومة وموازناتها

اليوم، يتمتع ملايين الأشخاص بالقدرة على التقاط صور أو مقاطع فيديو عالية الوضوح بآلات تسعها جيوبهم. وبمنتهى السهولة يمكنهم مشاركة ما التقطوه مع الجمهور سواء كان بعيدًا أو قريبًا، فتنتشر مشاهداتهم عبر المكان والزمان بدون الخضوع لقيود الحدود واللغة.

بالنسبة للباحثين في مجال حقوق الإنسان، تغير هذه الأنماط الجديدة من سبل مشاركة المعلومات كيفية اكتشافنا للمعلومات ذات الصلة، كما تشدد على الحاجة للتحقق والشك الصحي البَنَّاء.

وبمقارنة الوضع الآن بما كان عليه منذ بضع سنوات وحسب، نجد أن هناك فرصًا هائلة تتأتى من وجود الكثير من البيانات من العديد من المصادر لدعم العمل في مجال حقوق الإنسان. يمكن للبيانات الرقمية أن تدعم التوثيق في مجال حقوق الإنسان من حيث العمق والاتساع والدقة والكفاءة.

أولًا، يمكن لذلك أن يوفر مصدرًا جديدًا لتأييد الأدلة بالنسبة للتوثيق التقليدي لأحداث معينة. عادةً ما تُصنف انتهاكات حقوق الإنسان وفقًا للحدث القائم. بالتسلح بمصادر البيانات الجديدة، ينمو كم التفاصيل التي يمكن كشفها عن حدث ما (مثال: يمكن التعرف على إجابات الأسئلة المتعلقة بمن وماذا وأين ومتى بشكل أكثر تحديدًا)، وينطبق الأمر ذاته على أثر تقصي الحقائق.

ثانيًا، وقد يكون ذلك هو الأمر الأكثر أهمية، تُوفر البيانات وحدة معيارية للقياس يمكن التقاطها وتصنيفها ومقارنتها عبر المجموعات وعلى مر الوقت، مما ييسر من عملية رسم خرائط التوجهات والأنماط، والتي تساعد بدورها على تسليط الضوء على أوجه الخلل الأكثر نظامية.

إنعاش الطرق التقليدية

لطالما ارتبط توثيق حقوق الإنسان بمقابلة الضحايا وشهود العِيان وبجمع الأدلة المؤيدة، بحيث يركز على حادثة أو حدث بعينه، والهدف هو اكتشاف ما حدث لمن وعلى يد من وأين ومتى وكيف حدث.

والإجابة عن هذه الأسئلة الستة عملية مباشرة إلى حد بعيد عندما تخل الحكومات بأحد الالتزامات السلبية (التزام بعدم فعل شيء ما). التعذيب والحبس التعسفي والحملات الأمنية على التظاهرات السلمية وعمليات الإخلاء القسري والتعقيم بغير رضا، جميعها أمثلة على ذلك. ولكن عادة ما تكون الإجابة عن الأسئلة (ماذا ولمن وعلى يد من وأين ومتى وكيف) أصعب كثيرًا حينما يتعلق الأمر بالالتزامات الإيجابية.

تستوجب الالتزامات الإيجابية من الحكومة فعل شيء ما، وقد يتضمن ذلك القيام بشيء ما برمته أو القيام به بصورة مختلفة. ويندرج عدد هائل من انتهاكات حقوق الإنسان – وبالتحديد تلك المتعلقة بالحقوق الاقتصادية والاجتماعية والثقافية – تحت الفئة الثانية. الاتجار بالبشر وسوء استغلال العمالة ووحشية الشرطة وسوء التغذية والتشرد والأمية والأمراض التي يمكن الوقاية منها، جميعها أمثلة على ذلك.

ومثل هذا النوع من الانتهاكات معقد وله جذور متأصلة، فهي لا تقتصر على حدث ما أو حادثة بعينها، ولكنها تنتج عن خلل نظامي يرتبط بطريقة تصميم القوانين والسياسات واللوائح وتنفيذها، وهو ما تحاول طرق التوثيق التقليدية جاهدة الكشف عنه. ولكن مثل هذا الخلل يمكن أن يتسبب فيه عدد كبير من الفاعلين والعوامل المؤثرة، مما يصعب من عملية تحديد المسئول.

وقد يسهم وجود مقاربة أوسع نحو التوثيق في إلقاء الضوء على الفاعلين والعوامل المؤثرة على القوانين والسياسات واللوائح ووقعها على المجموعات بطرق معينة.

دراسة الحالة

الاستخدام الأمثل للبيانات من سوريا لتوثيق الانتهاكات

في أبريل/ نيسان ٢٠١١، بدأت مجموعة من النشطاء السوريين في رصد انتهاكات حقوق الإنسان وتوثيقها نظاميًّا عن طريق جمع ومشاهدة مقاطع فيديو على الإنترنت للعنف والفظائع المرتكبة. وعندما اختُطف عدة أفراد من الفريق، صممت البقية على تحسين أمنهم وطرقهم ومجموعات البيانات الخاصة بهم من خلال المشاورات مع الخبراء.

وانتهى بهم الأمر إلى تطوير منظمة غير هادفة للربح تسمى **مركز توثيق الانتهاكات**، تقوم الآن على جمع البيانات المتعلقة بالسجن والتعذيب والمدنيين المفقودين والقتلى والثوار وقوات النظام في سوريا باستخدام طرق التحقق شديدة الدقة، وذلك حتى يتسنى استخدام هذا التوثيق في مجريات العدالة الانتقالية حين ينتهي النزاع.

ولديهم فئات أكثر تفصيلًا في قاعدة البيانات والمزيد من الخيارات لتنقية البحث، كما أنهم يستخدمون صور الأقمار الصناعية بشكل أفضل لأغراض التحقق. يقول أحد ممثلي المركز: «الآن تُستخدم معلوماتنا بصورة سرية من قِبل ممثلي الأمم المتحدة والحكومات والمناصرين من جميع أنحاء العالم، بما أننا متأكدون من أن بياناتنا كاملة».

من أجل أن تكون أي بيانات مفيدة لتوثيق حقوق الإنسان، تحتاج إلى أن تكون قادرًا على عرض المكان الذي جاءت منه، وتوقيت إنشائها، والمسئول عن إنشائها والسبب من وراء ذلك.

المكان، الزمان، الشخص، الدافع.

دراسة الحالة

التحقيق في عمليات القتل الجماعي في بوروندي

اختفت جثامين ما لا يقل عن ٧٠ شخصًا أعدمتهم القوات الحكومية في بوروندي في ديسمبر/ كانون الأول ٢٠١٥ بشكل غامض مما أدى لتردد شائعات عن قبور جماعية. قضى أحد الباحثين الميدانيين لدى منظمة العفو الدولية عشرة أيام فيما بين التقاط الصور ومقابلة شهود العِيان بعد عمليات القتل، ولكن كانت هناك حاجة للمزيد من الأدلة. في الأغلب ستتمكن صور الأقمار الصناعية من المساعدة في تحديد موقع المقبرة، ولكن ذلك يكون في حالة معرفة المنطقة التي ينبغي البحث فيها من الأساس. ولحسن الحظ، تلقت العفو الدولية مقطع فيديو من أحد المعارف في بوروندي يظهر موقع الدفن المزعوم. تمت الاستعانة بجوجل إيرث على الإنترنت للحصول على الإحداثيات الدقيقة، وفي نهاية المطاف، أظهرت صور الأقمار الصناعية بالفعل عدم استواء التربة في النقطة المُعينة.

حازت عملية العثور على المقبرة الجماعية عبر القمر الصناعي على تغطية إعلامية هائلة، وساعدت في خلق ضغط سياسي. منذ عشرة أعوام، لم تكن العفو الدولية لتتحصل على مثل هذا المقطع، لأن الناس في بوروندي لم يكن لديهم هواتف محمولة بكاميرات، ولكن الآن، بفضل التطور التكنولوجي، يتمتع المحققون بالمزيد من الأدوات التي يمكن دمجها في عملهم الميداني التقليدي.

الصورة: صور الأقمار الصناعية تظهر عدم استواء التربة في منطقة بورينجا، بما يتوافق مع روايات الشهود وتسجيلات الفيديو الخاصة بالمقابر الجماعية. ©DigitalGlobe٢٠١٦

متى تستخدم البيانات الرقمية؟

إذا ما كنت أكثر اعتيادًا على طرق البحث والتوثيق التقليدية، فقد يبدو تحديد ما إذا كانت البيانات الرقمية أو محتوى وسائل التواصل الاجتماعية جديرَين باهتمامك كأمر عويص.

هذا القسم يطرح ستة أسئلة لمساعدتك في تحديد صافي قيمة الأنواع الأحدث من البيانات في سياق بحثك الخاص. هل ستساعدك حقًا؟ نحتاج إلى موازنة المزايا والعيوب باستمرار، بما يتضمنه ذلك من تكاليف وتوفير، وكذا **المخاطر المتعلقة بإساءة التصرف في البيانات**. على سبيل المثال، يمكن لخطر المراقبة أن يجعل من جمع البيانات الرقمية فعلًا غير مستحب في بعض السياقات، أو ربما لا يمكنك الحصول إلا على بيانات بعض المجموعات السكانية دون الأخرى مما يفسد نتائج استقصائك.

في الواقع، لا يختلف الأمر عن طرق البحث التقليدية إلى هذه الدرجة. يتمثل الجزء الأصعب في التفكير المبتكر في أي من البيانات يمكن أن تكون موجودة (وعلى وجه التحديد البيانات التي أنشئت لأغراض أخرى) وتقييم ما إذا كان بإمكانك وفريقك جمعها والتصرف فيها على نحو فعال.

سبعة أشياء لا بد وأن تضعها في الحسبان قبل استخدام البيانات الرقمية لحقوق الإنسان

١. هل ستساعد البيانات الرقمية بشكل حقيقي في الإجابة عن أسئلتك البحثية؟ ما هي مميزات وعيوب هذا المصدر أو الوسط بعينه؟ ما الذي يمكنك أن تتعلمه من الاستخدامات السابقة للتكنولوجيا ذاتها؟

٢. ما هي المصادر التي على الأغلب ستجمع أو تلتقط أنواع المعلومات التي تحتاجها؟ ما هو السياق الذي يتم إنتاجها واستخدامها فيه؟ هل سيتقبل الأفراد أو المنظمات الذين تركز عليهم في عملك هذه الأنواع من البيانات؟

٣. إلى أي مدى سيسهل دمج أنواع البيانات الجديدة في مجرى عملك القائم؟ هل لديك الوقت والمال الكافيان على أرض الواقع لجمع هذه البيانات وتخزينها وتحليلها، والأهم: التحقق منها؟ هل يمكن لأي من أفراد فريقك دعم التكنولوجيا بلا عوائق؟

٤. من يمتلك البيانات التي ستستخدمها أو يتحكم فيها؟ الشركات أم الحكومة أم الخصوم؟ ما مدى صعوبة الحصول عليها؟ هل طريقة الجمع عادلة أو قانونية؟ ما هو الموقف الداخلي من هذا الأمر؟ هل تحصلت على موافقة مستنيرة حقيقية من الأفراد؟

٥. كيف ستؤثر الفوارق والتقسيمات الرقمية فيما يتعلق بالدخول إلى المنصات الإلكترونية أو الحواسب الآلية أو الهواتف محليًّا على تمثيل المجموعات السكانية المختلفة؟ هل ستعزز الاستخلاصات المبنية على البيانات من أوجه عدم المساواة أو الصور النمطية أو مناطق عدم الوعي؟

٦. هل البروتوكولات التنظيمية فيما يتعلق بالسرية والأمن في التواصل الرقمي ومعالجة البيانات تكفي لتغطية المخاطر التي تتعرض لها أنت وشركاؤك ومصادرك؟ هل يتم تحديث أدوات الأمن وعملياته بما يكفي؟

٧. هل توجد إجراءات احترازية قائمة فيما يتعلق بمنع أي صدمة ثانوية قد تتعرض لها أنت أو شركاؤك بسبب مشاهدة المحتوى الرقمي على المستويَين الشخصي والتنظيمي أو التعامل معها؟

أمثلة عملية

إليك بعض الأمثلة الافتراضية التي تظهر مجموعة متنوعة من مصادر البيانات الرقمية واستخداماتها

السيناريو:

لاجئون محرومون من الرعاية الصحية | هل نستخدم البيانات الرقمية؟

أنت ترغب في التحقيق في ادعاءات بشأن حرمان اللاجئين المتنقلين من الرعاية الصحية، وتفكر في استخدام صور الأقمار الصناعية لرسم خرائط حديثة لطرق السفر ومحتوى وسائل التواصل الاجتماعي للعثور على شهادات وأفراد جاهزين للمقابلات. لديك ميزانية محدودة للغاية ولم تستخدم هذا النوع من البيانات من قبل، ولكنك تعرف أن معظم اللاجئين يمتلكون هواتف محمولة ويستخدمون وسائل التواصل الاجتماعي لمشاركة المعلومات. أكثر ما يُقلقك هو أن تقع بيانات الموقع في أيدي المجموعات الأمنية المحلية التي تهاجم المهاجرين. في الواقع، بسبب هذه المجموعات المحلية، بدأ اللاجئون بشكل مضطرد في نقل اتصالاتهم من المنصات الأكثر علنية مثل تويتر إلى مجموعات مغلقة للدردشة على الفيسبوك والواتساب.

ماذا تفعل؟

تقرر أن تبحث عن وسيلة للدخول إلى مجموعات وسائل التواصل الاجتماعي المغلقة من خلال معارفك، وأن تجعل من أمن كل من تتواصل معه على الإنترنت أولى أولوياتك. تستعلم من الأفراد والمجموعات عن الحرمان من الرعاية الصحية. في الوقت الحالي، تعدل عن استخدام الصور الجوية.

سؤال البحث:
هل يُحرم اللاجئون من الحصول على الحقوق الصحية في البلد س؟

الحكومة س هي نقطة دخول اللاجئين إلى الاتحاد الأوروبي. ظهرت تقارير بشأن انتهاك حق الحصول على الرعاية الصحية للاجئين الذين يدخلون الدولة على ظهر المراكب. تفترض دراسة الحالة تلك أن الباحث لا يعرف على وجه التحديد مكان دخول اللاجئين للبلد.

انتهاكات حقوق اللاجئين الصحية

أنواع من البيانات المحتملة

- بيانات الأقمار الصناعية
- بيانات وسائل التواصل الاجتماعي د
- قواعد البيانات الجغرافية المكانية
- معلومات الهوائيات غير التابعة للأقمار الصناعية
- معلومات الطقس
- البيانات المفتوحة أ
- معلومات الموازنة الحكومية هـ
- المعلومات المعهدة جماعيًا ب
- معلومات بيانات وسائل التواصل
- عينة عشوائية من البيانات من المراكز الطبية ج
- أنواع البيانات المحتملة و

أ. من المنظمات الإنسانية والشركاء المحتملين الآخرين (مثل معلومات الرعاية الصحية، تحليلات تقديم الخدمة، إلخ...).

ب. مثل خرائط إبلاغ المواطنين عن الأحداث المتعلقة باللاجئين عند نقاط الدخول)

ج. الإرشادات التي توفر الدعم الطبي للاجئين.

د. (على سبيل المثال مجموعات الفيسبوك أو الواتساب التي يستخدمها اللاجئون للتواصل فيما يتعلق بالدعم على الطريق أو المخاوف الأمنية).

هـ. فيما يتعلق بمخصصات الدعم الطبي للاجئين.

و. بيانات التيارات المحيطية أو العوامل الأخرى التي قد تؤثر على حركة اللاجئين.

السيناريو:

تتبع الرقابة على الإنترنت | هل نستخدم البيانات الرقمية؟

أنت تعمل في بلد من المعروف فيه أن الحكومة توقف الإنترنت عند خروج المظاهرات وحدوث القلاقل الاجتماعية، وتريد أن توثق ذلك. تكتشف أنه بإمكانك الدخول إلى سجلات جوجل لقطع الخدمة على الإنترنت، مما سيسمح لك بالتعرف على أوقات توقف الخدمة المحتملة، والتي يمكن إسنادها ترافقيًّا مع مصادر إضافية أخرى للبيانات، ولكن الحكومة بارعة في المراقبة رقميًّا وعلى الإنترنت، ويمكنها أن تتتبع نشاط متصفحك وتاريخ بحثك لتصل إليك وتتعرف عليك كناشط حقوقي.

ماذا تفعل؟

بالأخذ في الاعتبار تاريخ الحكومة في المراقبة، دربتك منظمتك على استخدام الـVPNs (الشبكات الافتراضية الخاصة) للبحث والتواصل عبر الإنترنت. تقرر أنه بإمكانك إخفاء آثارك الإلكترونية بما يكفي لتقوم بعملك البحثي بالرغم من المخاطر.

سؤال البحث:
هل انتهكت حكومة البلد ص حرية التعبير وحق الحصول على المعلومات بمنعها الدخول على الإنترنت؟

كانت هناك موجة من المظاهرات الشعبية في البلد ص على مدار العام الماضي. ومؤخرًا تأجج الموقف بعد أن أغلقت مظاهرة ضخمة قلب العاصمة. صرح نشطاء بأن الحكومة قد حظرت الإنترنت لكبح جماح المظاهرات ولمنع المعلومات من الوصول إلى الفاعلين خارج البلاد.

انتهاكات حقوق الإنترنت

أنواع من البيانات المحتملة

- سجلات الشركات المقدمة لخدمات الإنترنت
- إحصائيات حركة المرور على الإنترنت د
- التقارير الإعلامية
- وسائل التواصل الاجتماعي
- سجلات تحميل التطبيقات الجديدة أ
- سجلات الهاتف ه
- تحليل سرعة الإنترنت
- الحكومة تمنع الدخول على الإنترنت و
- البيانات الصادرة عن الشركات الخاصة ب
- بيانات سيفون
- طلبات الإزالة أو إغلاق حسابات المستخدمين ج

أ. وبالتحديد تلك التي تعتبر آمنة ومتاحة.

ب. واتساب ومنظمات حقوق الإنسان.

ج. التي تُبَلغ عنها وسائل التواصل الاجتماعي أو الشركات بشكل عام وعلى مواقع معينة.

د. تويتر، فيسبوك، إلخ...

ه. بيانات استخدام الهواتف المحمولة.

و. لكبح جماح المظاهرات.

السيناريو:

انتهاك حق الحصول على المياه | هل نستخدم البيانات الرقمية؟

تُظهر الصور الجوية للأنهار في منطقة بعينها ما يبدو وكأنه عوائق فعلية تحول دون الحصول على المياه، وبما أن هذه الأنهار تمثل المصدر الرئيسي للمياه بالنسبة للسكان المحليين، يساورك القلق بشأن انتهاك الشركة لحقوق السكان في الحصول على المياه. السكان الذين يعيشون على ضفاف الأنهار عادة ما يكونون أكثر فقرًا، بالرغم من أن معظمهم يمتلكون هواتف محمولة. تود أن ترسل استقصاءً عن طريق خدمة الرسائل القصيرة لتسأل إذا ما كان هناك تحديد لحقهم في الحصول على المياه وأين يحدث ذلك الأمر، ولكن هؤلاء السكان كانوا مستهدفين بشكل كبير في سياق أعمال التنمية خلال السنوات الماضية، وكما تناهى إلى سمعك، فإنهم يعانون بشكل أو بآخر من إجهاد الاستقصاءات. منظمتك غير الحكومية شابة ومواردها محدودة.

ماذا تفعل؟

بالرغم من أن خدمة الرسائل القصيرة سوف تمكنك من الوصول إلى السكان المستهدفين، فربما يمنعك السياق من الحصول على استجابات. وبافتراض: (١) أنك تستهدف سكانًا أفقر ويعانون من إجهاد الاستقصاءات، (٢) أنه سيتعين عليك أن تطلب من كل مستجيب دفع تكلفة الرسائل بنفسه، (٣) أن اسم منظمتك ليس معروفًا بالدرجة الكافية، فإنك تدرك أن الأمر قد يمثل مهمة شاقة. تقرر أن تطلب من أحد الزملاء في إحدى المنظمات غير الحكومية المعروفة تقديمك لأحد قادة المجتمع حتى يتسنى لك شرح مشروعك وطلب مدخلات المجتمع فيما يتعلق بتصميم الاستقصاء والتوصل إلى الكيفية التي سيمكنك بموجبها توفير المعلومات بشأن مشروعك الناشئ للمجتمع.

سؤال البحث:
هل إفباور مسئولة عن تلوث إمدادات المياه؟

في البلد س توجد مستويات مرتفعة لسوء التغذية بين أطفال الأسر منخفضة الدخل بسبب الدوسنتاريا. كما توجد العديد من العمليات التجارية لزراعة الزهور بالقرب من الأنهار في كافة أنحاء البلاد. تمتلك معظم المزارع شركة واحدة متعددة الأنشطة: إفباور. يوجد اثنان من أعضاء مجلس إدارة إفباور على صلة قرابة مباشرة بوزراء في الحكومة.

انتهاك الحق في الحصول على المياه

أنواع من البيانات المحتملة

- الصور الفوتوغرافية أو التي تلتقطها الأقمار الصناعية أ
- إحصائيات الصحة الوطنية
- تحليلات البيانات/ البحث على الإنترنت
- البيانات الموازنية ب
- معلومات موقع العمل وعملياته
- بيانات تقديم الخدمة ج
- استقصاء عن طريق خدمة الرسائل القصيرة بشأن استهلاك السعرات
- تحليل تلوث المياه
- تداخل البيانات الجغرافية والوقتية

أ. صور الزوال الزمني أو الصور الجغرافية المكانية.

ب. الإنفاق الحكومي على برامج التغذية.

ج. الحكومة أو الوكالات الإنسانية.

الحصول على الدعم التنظيمي

حتى بوجود الرغبة في التغيير، قد تتسبب الساعات الطويلة والميزانيات المحدودة في استمرار التزام المنظمات والأفراد بالنموذج القديم لفعل الأشياء. وبالتالي، فمن أجل دمج ممارسات البيانات الحديثة، لا بد وأن تعلي إدارة المنظمة من قيمة التغيير. إليك عشر نقاط يمكن تضمينها في المناقشات مع المديرين لمساعدتهم على رؤية ضرورة التغيير.

١. **واقع السوق:** العديد من منظمات حقوق الإنسان تعمل بالفعل باستخدام البيانات الرقمية، ولكن الكثير من هذه المنظمات تفعل ذلك بدون الاستثمار في عملية الإلمام بالبيانات. الفشل في تطوير المهارات الداخلية اللازمة للمنظمة قد يعرض أهمية عملك للخطر.

٢. **الميزانية:** العديد من الأدوات المقترحة في هذا الدليل منخفضة التكلفة أو مجانية.

٣. **التدريب:** نعم، يستغرق التدريب وقتًا، ولكن الموظفين يُقدرون التدريب. تظهر الأبحاث أن تقدير الموظفين لفرص التدريب الجديدة في العمل يحل في المرتبة الثانية مباشرة بعد المكافأة المالية. بالتحديد للمنظمات الصغيرة، فإن الاحتفاظ بالعاملين وتقليل دوران الموظفين يعدان أمرين حيويين. توفر أماكن مثل School of Data (سكول أوف داتا) أو Advocacy Assembly (آدفوكاسي آسمبلي) دورات مجانية على الإنترنت.

٤. **اجتذاب الموظفين الجدد:** يساعد ظهور المنظمة بشكل مستشرف للمستقبل واستخدامها للأدوات الجديدة على اجتذاب أفضل الموجودين في المجال.

٥. **الأثر:** يمكن لاستخدام البيانات الجديدة بشكل فعال أن يحسن من النتائج وأن يتيح رصدًا أفضل لانتهاكات حقوق الإنسان.

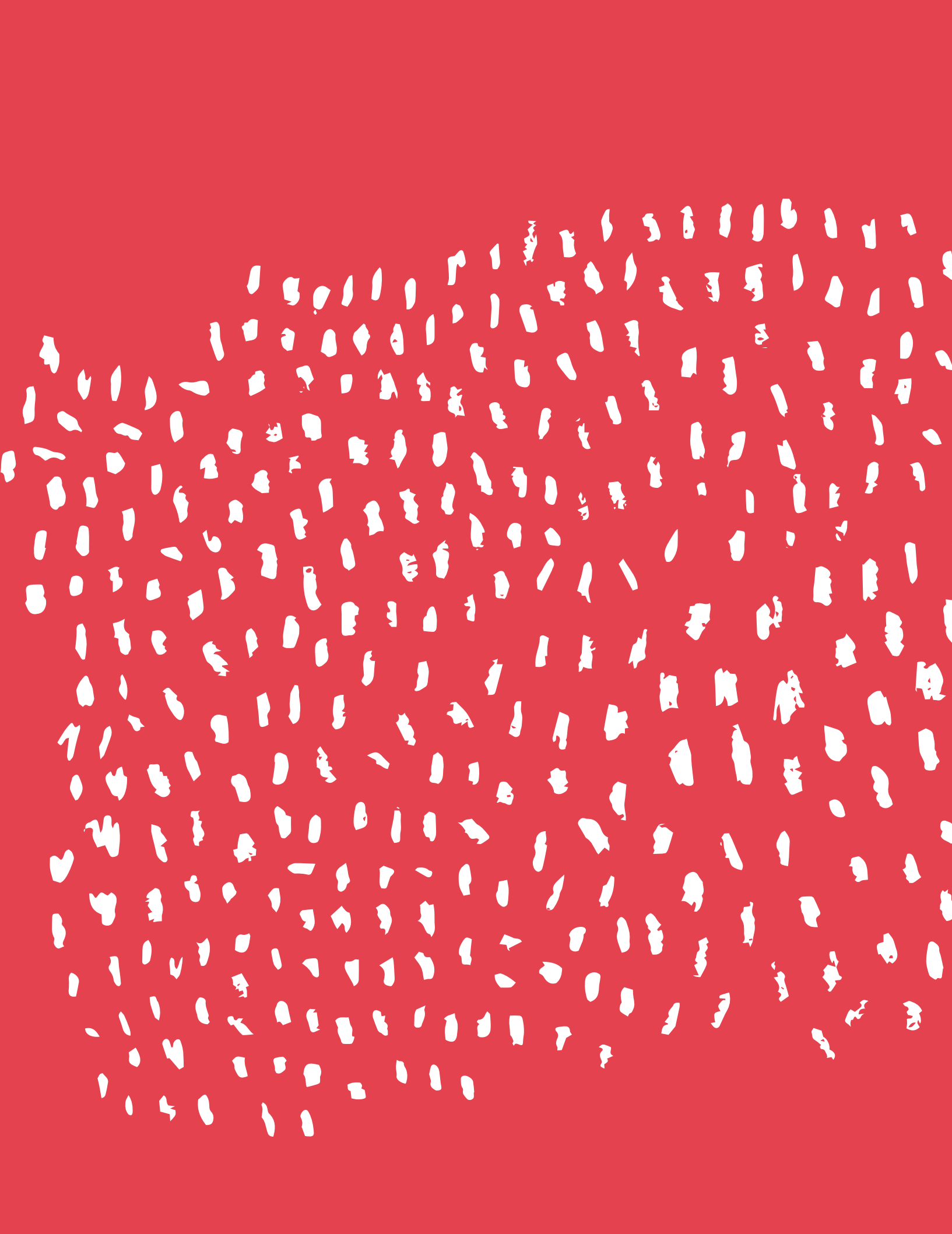
٦. **التمويل:** يحرص المانحون على ربط الدعوات الجديدة لتقديم مقترحات التمويل بالبيانات الرقمية واستخدامها في صياغة تقارير حقوق الإنسان.

٧. **الوسم:** يجعل المنظمة تبدو ذكية ومستشرفة للمستقبل وجاهزة للارتباط بالتطورات الجديدة والانخراط بها.

٨. **المهمة:** هي رصد انتهاكات حقوق الإنسان ورفع تقارير بشأنها وزيادة الوعي بها. عند استخدام البيانات الرقمية بشكل صحيح، فإنها تتيح للمنظمات فعل كل ذلك بشكل أفضل.

٩. **أحاديث استراحة الغداء:** ادع شخصًا يستخدم البيانات الرقمية في عمله بنجاح لإعطاء كلمة حول ما يقوم به.

١٠. **بناء شبكات النظراء:** ابنِ علاقات مع المنظمات النظيرة ذات التوجه البياناتي لمشاركة الممارسات المثلى.



فهم التحقق والتوثيق

ما هي الميتاداتا (البيانات الخلفية)؟

الميتاداتا هي المعلومات الخاصة بالملف (مثل ملفات الوورد أو البي دي إف أو الصور أو الموسيقى، إلخ...) المخزنة بداخل الملف ذاته، والمختفية عن الأنظار.

يمكن لهذه المعلومات أن تتضمن وقت إنشاء الملف وتاريخه، واسم المستخدم الخاص بمن أنشأه أو عدَّله، ومعلومات حول الجهاز الذي استخدم لإنشائه وأنواعًا أخرى من المعلومات، وذلك يعني أن الميتاداتا الخاصة بالملف يمكنها أن تكشف عمّن أنشأه. تتولد هذه المعلومات أوتوماتيكيًّا من الأجهزة مثل الكاميرات والحواسب الآلية والهواتف، ولكن أيضًا يمكن لمن يعرفون كيفية التلاعب بها فعل ذلك، ويمكن لذلك أن يكون شيئًا جيدًا إذا ما أردت أن تكون المعلومات سرية عند مشاركتك للملفات، ولكن المخاطر لا تخفى عليك إذا ما كنت تتعامل مع التحقق من المعلومات الحقوقية الحساسة.

لنأخذ الصور كمثال. ماذا يحدث عندما تلتقط صورة بكاميرا رقمية؟ إذا ما كانت الكاميرا أو الهاتف يعرفان موقعك، فإن هذه المعلومات (في صورة إحداثيات نظام تحديد المواقع عالميًّا GPS) يمكن أن تُسجل في الميتاداتا الخاصة بالملف. إذا ما كانت الكاميرا تعلم الوقت، فإنها تسجل التاريخ والوقت الذي التقطت فيه الصورة. إذا ما كانت الكاميرا أو الهاتف لديهما رقم مسلسل، فيمكن أن يكون هو أيضًا مسجلًا في الميتاداتا. تحتوي صيغ ملفات الصور الرقمية مثل التيف (TIFF) (صيغة ملف الصور الموسومة) والجيه بيه إي جي JPEG التي تنشئها الكاميرات الرقمية أو الهواتف الذكية على الميتاداتا في صورة صيغة تُسمى إكسيف (EXIF) (صيغة ملف صوري متبادل) يمكن أن تتضمن كل المعلومات المذكورة عاليه، وحتى صورة مُصغرة للصورة الأصلية.

الملفات الأخرى مثل المستندات النصية تتضمن ميتاداتا أيضًا، قد تشتمل على طول المستند، ومُنشئه، ووقت تعديل المستند وملخص آلي قصير لمحتواه. يمكن لبيانات الإكسيف والنوعيات الأخرى من الميتاداتا أن تكون مفيدة للغاية لأغراض التحقق من الوسائط، وأيضًا من أجل إنشاء الكتالوجات وتنظيمها.

جلو الميتاداتا

في بعض الحالات، قد ترغب في إزالة الميتاداتا من الملفات المرتبطة بانتهاكات حقوق الإنسان. وتزداد أهمية هذا الأمر في الحالات التي تمثل فيها مشاركة الأدلة على انتهاكات حقوق الإنسان أو نشرها خطرًا عليك أو على الآخرين المشتركين في تسجيل الواقعة.

يمكن استخدام عدد من البرمجيات والأدوات الموجودة على الإنترنت «لجلو» الميتاداتا من الملفات. بينما لا يمكن إزالة جميع أنواع الميتاداتا – مثل حجم الملف أو أبعاد الصورة أو وقت تعديلها – فإن الميتاداتا المتعلقة بمن أنشأ وعدّل الملف عادةً ما يمكن إزالتها. تتباين كفاءة الأدوات المستخدمة، لذا فمن الأفضل تجربة أداتين مختلفتين والتأكد من أن الميتاداتا قد أزيلت بنجاح.

إذا ما كنت تعمل مع مراسل موثوق به، فقد يمكنك أن تقترح عليه إلغاء خاصية خدمات الموقع (بيانات الـGPS) على جهازه من أجل إخفاء هويته. لا بد من التحلي بالحذر عند طلب الصور، لأن طراز الهاتف أو معلومات الإكسيف الأخرى يمكن استخدامها لتعيين مواقع مصادرك.

يحتوي دليل Security in a Box (عدة الأمان) من Tactical Technology Collective (تكتيكال تكنولوجي كوليكتيف) وFront Line Defenders (فرونت لاين ديفيندرز) على المزيد من المعلومات بشأن إزالة الميتاداتا.

تحقق، ثم تحقق، ثم تحقق

البيانات من أي نوع – حتى المواد التي جمعتها بنفسك – تتطلب تحققًا متعمقًا لكي تحمي سمعتك والأشخاص على الأرض من الضرر. من الأهمية بمكان أن تقارب كل قطعة من المحتوى بعين نقدية، حتى لو كنت تتمنى أن تكون حقيقية.

يجب أيضًا أن تتقبل حقيقة أنه لا توجد طريقة واحدة تضمن التحقق. التحقق هو عبارة عن عملية تمنحك والآخرين الثقة في صدقية المحتوى. يجب أن تتمتع بالشفافية بشأن ما لا تعرفه مثلما هو الحال بالنسبة لما تعرفه، وذلك لمصلحة الجميع.

في البيئات شديدة الضغوط منخفضة الموارد، عادةً ما تُهمش عملية التحقق من البيانات الرقمية، بدلًا من كونها بندًا تتضمنه خطط البحث منذ البداية. إذا ما ساورتك الشكوك بشأن كيفية التحقق من نوعية معينة من المحتوى، فالأكثر أمانًا هو استشارة الخبراء للحصول على المساعدة.

خمس خطوات نحو التحقق

١. كيف حصلت على المحتوى؟

فكر في قنوات المعلومات التي سافر خلالها المحتوى قبل أن يحط على مكتبك. كم مرة تداولته الأيدي؟

٢. من أنشأ المحتوى؟

هل الشخص الذي شارك أو رفع المحتوى على الإنترنت هو نفسه من أنشأه؟ أم أنه شخص آخر؟ اسْأَلْ إذا لم تكن تعرف.

٣. من أين يأتي المحتوى؟

يمكن تزوير الأوصاف والميتاداتا بسهولة. هل من ثمة معالم أو أصوات (مثل سرينة الشرطة أو اللكنات) يمكنها مساعدتك على التحقق من الموقع؟

٤. متى أُنشئ المحتوى؟

لا يمكنك أن تثق في ختم التاريخ الموجود على الملف. هل هناك أدلة بصرية مثل الطقس؟ يمكن لعملية البحث العكسي عن الصور أن تكشف إذا ما كانت الصورة تظهر في مكان آخر.

٥. لماذا أُنشئ المحتوى؟

هل بإمكانك تحديد الهدف من وراء مشاركة المحتوى؟ ما هي مصالح مَن رفعه؟

التحقق

التحقق، لماذا؟

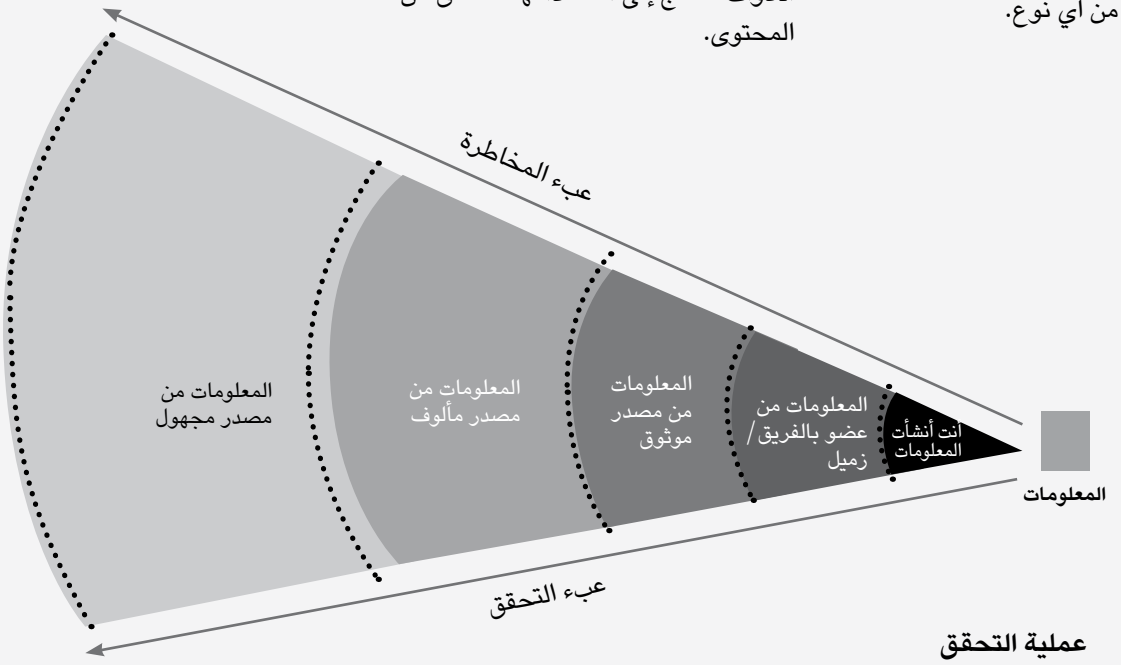
قد يبدو الأمر جليًّا، ولكن ما لم تكن تعمل باستخدام مواد قمت أنت بجمعها بنفسك، أو ملحوظاتك الخاصة، فمن الأهمية بمكان أن تتحقق من أن المعلومات التي تستخدمها، هي في الواقع، ما تدعي كونها عليه. المخاطر المتعلقة بالسمعة، بالإضافة إلى المخاطر على الأفراد موضوع البحث تستلزم العناية الواجبة عند استخدام البيانات الجديدة من أي نوع.

خطوات التحقق:

التحقق عملية متغيرة باستمرار، والمنتج النهائي نادرًا ما يكون باتًّا. هي على الأحرى عملية تضفي الثقة على المعلومات. قد تزعم هذه المعلومات شيئًا يختص بالإجابات عن أسئلة من وما وأين ومتى المتعلقة بحدث معين.

طرح هذه الأسئلة ذاتها بشأن المعلومات نفسها هو جزء من عملية التحقق. التفكير في هذه الأسئلة سوف يُعرِّف أي الأدوات تحتاج إلى استخدامها للتحقق من المحتوى.

ما هو المصدر؟
مَن رفع المحتوى أو شاركه؟
أين أُنشئ المحتوى؟
متى أنشئ المحتوى؟
لماذا أنشئ المحتوى؟



عملية التحقق

تدريب:

تحقق من هذا الفيديو على يوتيوب

أنت باحث حقوقي، وتحتاج إلى التحقق من فيديو على اليوتيوب [https://youtube/clrICxJihWI] عن استخدام القوة المفرطة من قِبل الشرطة ضد مظاهرة في ريو دي جانيرو بالبرازيل، والذي شاركه أحد زملائك معك.

١. تقوم **بتحميل الفيديو** للحفاظ عليه، لأن المحتوى الإلكتروني الحساس عادةً ما تتم إزالته.

٢. باستخدام You Tube data Viewer (مُشاهد بيانات اليوتيوب)، تتعرف على توقيت النشر (ولكن ليس توقيت التسجيل)، وهو ٥:٣٠ مساءً (بتوقيت برازيليا) في ١٤ أبريل/ نيسان ٢٠١٤. لا يُظهر البحث العكسي عن الصور المصغرة للفيديو أي نسخ سابقة من الفيديو على الإنترنت.

٣. أورد المُنشئ، كمساعدة، اسمه تحت الفيديو، وتستنتج من خلال النظر إلى منصات وسائل التواصل الاجتماعي الأخرى أن من رفع الفيديو يبدو وكأنه ناشط في ريو دي جانيرو.

٤. يزخر الفيديو والوصف بالأدلة عن الموقع (مجلس المدينة بريو دي جانيرو). وللتحقق، تستخدم الخريطة الإلكترونية Wikimapia (ويكيمابيا) لتعثر على مجلس مدينة ريو، كما تستخدم صور القمر الصناعي الموجودة على جوجل إيرث للإسناد الترافقي للمعالم المرئية (مبنى إداري، جسر المشاة). الصور المسندة ترافقيًّا من بانوراميو (يمكن الدخول عليه من خلال جوجل إيرث) تظهر تطابقًا أيضًا.

٥. يقول الوصف إن المظاهرة قد خرجت صباح الاثنين تحت أمطار غزيرة. تتطابق بيانات الطقس التاريخية التي تحصل عليها من خلال WolframAlpha.com مع ما يظهر في الفيديو (طقس ممطر وضبابي)، مما يزيد من مصداقية الفيديو والتوقيت المزعوم لتسجيله.

٦. تستخدم خاصية تشغيل الفيديو بالتصوير البطيء (على اليوتيوب أو مشغل الوسائط VLC لتنظر عن كثب إلى الزي الشرطي وشاراته، مقارنةً بتلك التي تراها على موقع الشرطة الرسمية، تدون التفاصيل احتياطيًّا في حال ما احتجت إليها في المستقبل فيما يتعلق بالتحقيقات مع الأفراد المتورطين.

٧. أخيرًا، عندما تبحث عن المحتوى الإضافي باستخدام محرك بحثك المعتاد، تستطيع أن تجد المزيد من مقاطع الفيديو الأخرى التي تعود لنفس التاريخ ونفس المظاهرة [https://youtube/sxyrP0yBBts] كبرهان إضافي على الفيديو.

كيفية التحقق من الصور باستخدام ملفات الإكسيف (سؤال وجواب)

كل صورة رقمية تتضمن ملفًا للميتاداتا يُسمى إكسيف بإمكانه تعريف توقيت ومكان التقاط الصورة. تضاف هذه المعلومات إلى الملف لحظة التقاط الصورة بغض النظر عن الجهاز المستخدم. يمكن لملفات الإكسيف أن تكون مفيدة للغاية في عملية التحقق، ولكن يمكن أيضًا التلاعب بها عند تداول الصورة أو نشرها عبر وسائل التواصل الاجتماعي.

متى يجب أن أبحث عن ملف الإكسيف؟

يجب على الصورة أن تتضمن ملف الإكسيف إذا ما كانت قد جاءت مباشرة من كاميرا المصدر إلى صندوق بريدك بدون أن يتم تغييرها أو تداولها. يمكن أن يظل ملف الإكسيف موجودًا إذا ما تم تعديل الصورة. إذا لم تتضمن الصورة ملف الإكسيف فيجب أن تتشكك في أصالتها. يمكنك أن تنظر إلى ملف الإكسيف والبيانات الأخرى لترى أي نوع من الكاميرات أنشأها أو أي نوع من البرمجيات استُخدم لتصديرها. وإذا ما تم تغييرها أو التلاعب بها، فقد تحتوي على أنواع أخرى من الميتاداتا أيضًا.

هل ستكون بيانات الإكسيف موجودة دائمًا في صورتك؟

تزيل معظم منصات التواصل الاجتماعي بيانات الإكسيف أو تنشئ نسخًا أقل جودة من الصورة عند رفعها على المنصة (باستثناء مواقع مشاركة الصور المتخصصة). إذا ما كنت تتحقق من صورة مصدرها وسائل التواصل الاجتماعي، فلن تجد عادةً أيًّا من بيانات الإكسيف.

كيف أجد بيانات الإكسيف؟

إذا ما بحثت على الإنترنت عن «EXIF data viewer» مشاهد بيانات الإكسيف فسترى العديد من الخيارات. إحدى أبسط الأدوات هي Jeffry's EXIF Data Viewer *[http://regex.info/exif.cgi]* والتي توفر أيضًا برنامجًا مساعدًا لعدة متصفحات. يمكنك أيضًا أن تجد بيانات الإكسيف باستخدام البرامج الموجودة على حاسوبك مثل الفوتوشوب والآي فوتو.

هل يمكن التلاعب ببيانات الإكسيف؟

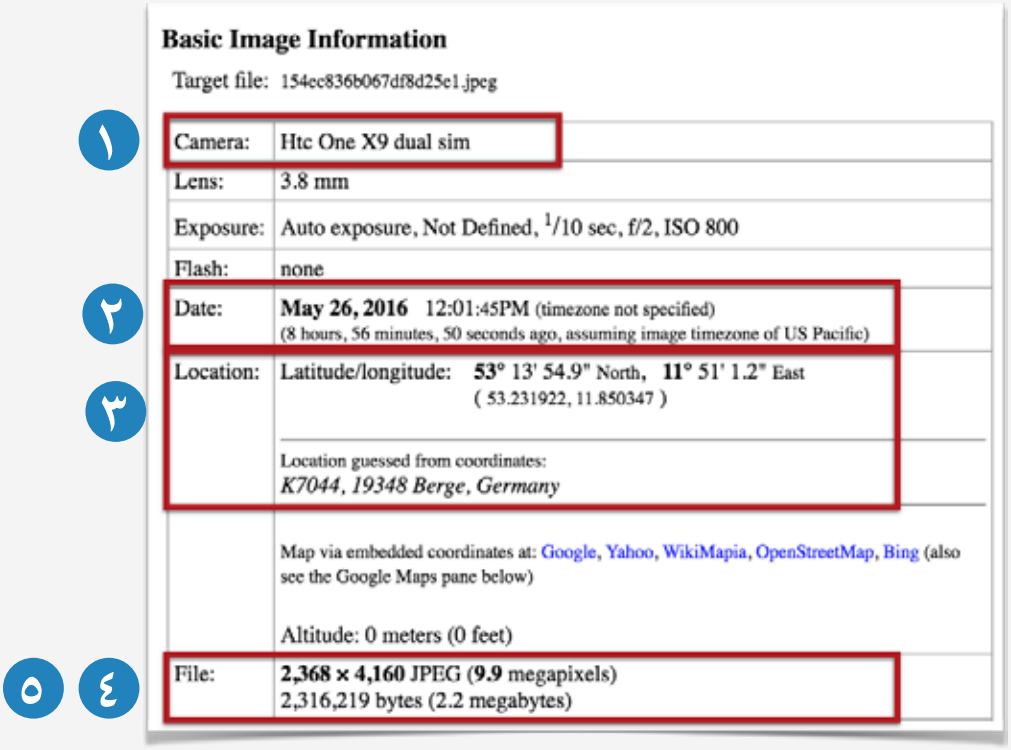
نعم. يمكن استخدام أدوات مثل Geosetter (جيو سِتر) وبرامج تعديل الصور الأخرى من أجل تزوير بيانات الإكسيف. وذلك يعني أن بيانات الإكسيف يجب أن تستخدم كواحدة من ضمن العديد من الخطوات في عملية التحقق خاصتك. يمكن لأدوات مثل JPEGSnoop أن تكتشف البرامج التي استُخدمت للتلاعب بالصورة.

ماذا لو التقط أحدهم صورة لصورة قديمة؟

تخبرك بيانات الإكسيف بالجهاز الذي التقط الصورة، ولكنها لا تعرف أي شيء عمّا كان أمام الكاميرا. حتى لو تطابق ملف الإكسيف مع التاريخ والموقع، فيمكن للصورة بالرغم من ذلك أن تكون غير ما تدعيه: مثلًا صورة لصورة.

في العمق

ما تقوله الصورة عنك...
هذا هو شكل ملفات الإكسيف



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)

١ ٢ ٣ ٤ ٥

بعض بيانات الإكسيف فقط هي الهامة بالنسبة لعملية التحقق.

١ **الكاميرا المستخدمة في التقاط الصورة:**

أي طراز الكاميرا أو الهاتف. إذا ما كنت، على سبيل المثال، تراسل شخصًا شارك إحدى الصور معك، فيمكنك أن تطابق ما تخبرك به بيانات الإكسيف بشأن الكاميرا المستخدمة في التقاط الصورة بما يخبرك به الشخص حول الجهاز الذي استخدمه لالتقاطها. إذا ما أعطاك معلومات مختلفة – بشأن الكاميرا أو الهاتف الذكي المستخدم– عمّا يظهر في ملف الإكسيف، فإن ذلك يعد جرس إنذار قويًّا.

٢ تاريخ التقاط الصورة وتوقيته:

هذا الأمر مهم من أجل التأكد من توقيت التقاط الصورة، ولكن الإكسيف لا يوضح المنطقة الزمنية. يمكنه أن يعكس إما التوقيت المحلي، وإما التوقيت العالمي المنسق، وفقًا للجهاز والإعدادات. بعض أنواع الكاميرات تتمتع بوسوم الميتاداتا الخاصة بها، والتي تكمل الإكسيف، وقد تشتمل على بيانات المنطقة الزمنية. يوجد أيضًا وسم إكسيف غير معياري لفروق التوقيت، ويمكنه توضيح فارق التوقيت بالمقارنة بتوقيت جرينتش. العديد من مواقع رفع الوسائط مثل اليوتيوب تتحول تلقائيًّا إلى توقيت الباسيفيكي في حالة عدم اشتمال الصورة على منطقة زمنية. يجب أيضًا أن تضع في حسبانك احتمالية أن تكون إعدادات الوقت والتاريخ على الجهاز غير صحيحة، وقد يكون هذا الاحتمال أكثر ورودًا في حالة استخدام الكاميرا أكثر من الهاتف الذكي لأن الأخير عادة ما يقوم بتحديث إعدادات الوقت والتاريخ بشكل تلقائي.

٣ تعداد البكسلات في الصورة:

كل كاميرا تلتقط صورها بأحجام مختلفة. على سبيل المثال، الآيفون ٥ ينتج صورة حجمها ٨ ميجابكسل، بينما ينتج سامسونج جالكسي إس ٥ صورة حجمها ١٦ ميجابكسل، في الرسم بالصفحة السابقة عن معلومات ملف الإكسيف، نجد أن الصورة حجمها ٩,٩ ميجابكسل، وذلك يعني ٢٣٦٨ * ٤١٦٠ بكسل (الميجابكسل الواحد = مليون بكسل). يجب أن تأخذ حذرك وتطرح أسئلتك على الشخص الذي أسهم بالصورة إذا ما كان تعداد البكسلات والأبعاد لا تتوافق والأحجام التي يدعمها الجهاز المزعوم.

٤ أبعاد بكسلات الصورة:

أبعاد البكسلات (العرض والطول) تساعد بطريقتين: أولًا، الكاميرات المختلفة التي تنتج صورًا بنفس تعداد البكسلات يمكنها أن تنتج صورًا بأبعاد مختلفة. على سبيل المثال، تنتج كاميرتا فوجي فيلم إكس تي-٢ ولايكا إم-دي تايب ٢٦٢ صورًا حجمها ٢٤ ميجابكسل، ولكن بأبعاد بكسل مختلفة. أبعاد البكسل لكاميرا فوجي فيلم إكس تي-٢ هي: ٦٠٠٠ * ٤٠٠٠ بكسل، أما كاميرا لايكا إم-دي تايب ٢٦٢، فإن أبعادها هي ٥٩٧٦ * ٣٩٩٢ بكسل.

كما أن أبعاد البكسلات يمكنها أن توفر أيضًا دليلًا على ما إذا كان قد تم قص الصورة. وكقاعدة عامة، يجب أن ينتج رقم صحيح عند قسمة عرض الصورة وطولها على ثمانية. غالبًا ما يتكون وضوح الكاميرات الرقمية من مضاعفات الرقم ٨، ويمكن التحقق من ذلك عن طريق مراجعة مواصفات الكاميرا التقنية. (توجد استثناءات لهذه القاعدة، وبالتحديد مع تطبيقات الهواتف المحمولة وخواص التصوير البانورامي).

٥ إحداثيات الجي بي إس لموقع التقاط الصورة:

إذا ما كان الجهاز المستخدم في التقاط الصورة يتمتع بإمكانيات الجي بي إس (عادةً ينطبق ذلك على الهواتف الذكية، ولكن بعض الكاميرات تتمتع بتلك الإمكانيات أيضًا)، وقام مُلتقط الصورة بتشغيلها، فقد تظهر بيانات الإكسيف إحداثيات الجي بي إس الخاصة بموقع التقاط الصورة. والحروف جي بي إس هي الحروف الإنجليزية الأولى من Global Positioning System أو نظام تحديد المواقع عالميًّا – وهو نظام لتحديد المواقع بالاستعانة بالأقمار الصناعية. في حالة وجودها، ستُظهر معظم برامج مشاهدة بيانات الإكسيف هذه الإحداثيات على خدمة الخريطة الإلكترونية.

استخدام بحث الصور العكسي للتحقق والتعرف

محركات بحث الصور أدوات رائعة للتحقق والتعرف. عندما ترفع صورة على محرك بحث الصور وتقوم بعملية «بحث الصور العكسي»، فإنه يبحث عن أسماء الملفات المطابقة أو الصور المماثلة التي تظهر على الإنترنت بالفعل. يمكن لذلك أن يساعدك على تحديد ما إذا كانت الصورة هي ما تحسبه، أم أنها أقدم مما اعتقدته أو ما إذا سبق استخدامها في سياق أو دولة مختلفَين.

١. **توصل إلى محرك البحث المناسب لك.**
TinEye (تين آي) وبحث جوجل الصوري يوفران أكثر قواعد البيانات شمولاً، ولكن يتمتع العديد من محركات البحث الأخرى (Bing (بينج) و Yandex (ياندكس) وBaidu (بايدو) أيضًا بخاصية بحث الصور العكسي. اختبرها لتعرف أيها الأفضل في السياق الجغرافي.

٢. **دائمًا ابحث مرتين.**
كل محرك بحث عكسي للصور يستعلم من قاعدة بيانات مختلفة، ويفهرس الصور الجديدة بسرعات مختلفة. قد تظهر صورك في أحد محركات البحث دونًا عن الآخر.

٣. **صنف نتائج بحثك بالأقدم أولًا.**
إذا ما كانت الصورة تنتمي لواقعة مختلفة عما يدعيه من أرسلها، سوف تُظهر هذه الخطوة التباين.

٤. **حدد المعالم جغرافيًّا.**
إذا ما كنت تحاول التعرف على أحد المعالم في صورة أو في فيديو، فإن محركات البحث التي تقدم خاصية «التماثل» (similar to) في البحث ستوفر لك مساعدة هائلة، لأن المعالم توثق بشكل كبير.

احذر: ليس بإمكان بحث الصور العكسي أن يخبرك بتوقيت التقاط الصورة. هو يخبرك فقط بما إذا كانت الصورة قد سبق إدراجها على الإنترنت ومتى حدث ذلك.

احذر: إذا لم تظهر صورتك في بحث الصور العكسي، فإن ذلك لا يعني بالضرورة أنها جديدة. يمكن لهذه الصورة أن تكون قد وصلت لك بعد سنوات من اختزانها على أحد الأقراص الصلبة.

دراسة الحالة

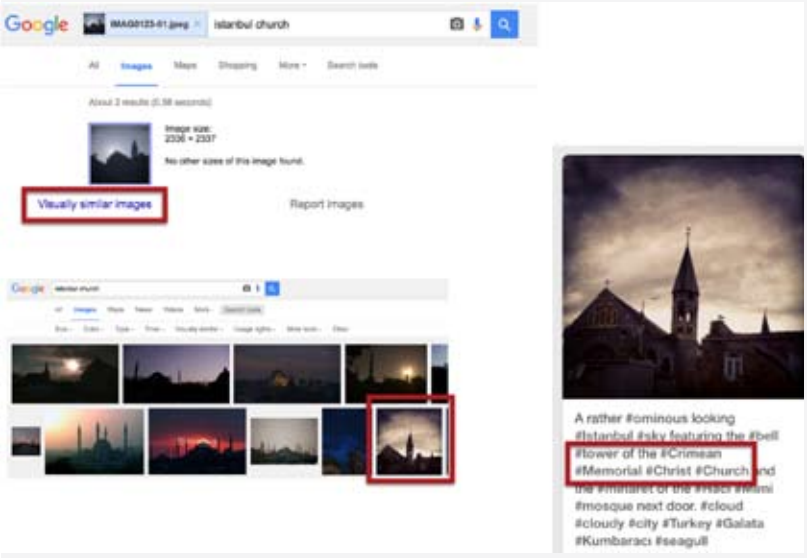
تحقق من موقع هذه الصورة

لدينا صورة لكنيسة يقال إنها من إسطنبول بتركيا.

للتحقق من هذا المَعْلم من خلال بحث الصور العكسي، نقوم برفع الصورة على صور جوجل ونكتب «كنيسة إسطنبول» مع الصورة.

لدينا خيار البحث عن صور «مماثلة بصريًا»، والذي يأخذنا لصفحة بها صورة يظهر فيها نفس البرج ونفس السقف. وبالضغط على هذه الصورة، نجد أنه من المقترح أن هذه الصورة تمثل كنيسة القرم بجالاتا بتركيا، والتي يمكننا الآن رؤيتها على الخريطة.

يمكنك أن تقوم بعملية التحقق ذاتها بالنسبة لمقاطع الفيديو. ببساطة، خذ لقطة من الشاشة لأحد المعالم في مقطع فيديو واتبع الخطوات نفسها.



بيانات وسائل التواصل الاجتماعي

في يونيو/ حزيران ٢٠١٤، نشرت إحدى الصحف مقطع فيديو لعملية إعدام غير رسمية في جمهورية أفريقيا الوسطى على الإنترنت، وانتشر بشكل كبير على وسائل التواصل الاجتماعي، ولكن بعد التحقق منه، اكتشفت العفو الدولية أن الواقعة حدثت في نيجيريا، وانتهى الأمر بأن أصبح هذا الفيديو أساس بحث منظمة العفو المعنون تورط الجيش النيجيري في جرائم الحرب.

يظهر هذا المثال المآزق وكذا الفرص الهائلة التي يمثلها محتوى وسائل التواصل الاجتماعي لأبحاث حقوق الإنسان. ففي أي صورة كان هذا المحتوى؛ سواء نص أو صور أو فيديو أو مقاطع صوتية، فإنه يتمتع بإمكانية الكشف عن الفظائع المخفية، وفي الوقت ذاته فقد يهدد سمعة المنظمة لو استخدم بإهمال. وبالإضافة إلى ذلك، فإن الكم الهائل من المحتوى الذي تتم مشاركته عبر المنصات المتعددة يمكن أن يغرق الباحثين، وفي بعض الأحيان يتطلب مهارات متخصصة في التنظيم والاكتشاف.

وسائل التواصل الاجتماعي مختلفة تمامًا عن الموارد التقليدية مثل شهادات شهود العيان أو الصحف، بالتحديد لأن المصدر الأصلي للمعلومات عادةً ما يكون غير واضح، ولأن المعلومات المغلوطة يمكنها أن تنتشر بسرعة شديدة من شخص واحد إلى الآلاف. في الوقت ذاته، تتزايد أهمية وسائل التواصل الاجتماعي، وحتى الحكومات والجيوش تستخدم القنوات الإلكترونية (بشكل حصري في بعض الأحيان) لتوزيع المعلومات إلى الجمهور مباشرة. تتضمن الأمثلة الحديثة تقارير الجيش الروسي الجارية بشأن العمليات العسكرية في سوريا على اليوتيوب، وبقوات الدفاع الإسرائيلي على الإنترنت بشأن العمليات في غزة في ٢٠١٤.

يمكن لمثالين أن يساعدا في شرح الفرص الهائلة لإعادة بناء الأحداث والتحقيقات طويلة الأمد. في مصر، أتاح محتوى وسائل التواصل الاجتماعي إعادة بناء مقتل متظاهرة سلمية على يد الشرطة في ٢٠١٥، مما أسفر عن تحقيق ومحاكمة. في نيجيريا، لعب محتوى وسائل التواصل الاجتماعي دورًا حاسمًا في توثيق جرائم الحرب في ٢٠١٤.

عندما يتمتع الباحثون بمهارة أكبر فيما يتعلق بطرح الأسئلة الخاصة بوسائل التواصل الاجتماعي وتوظيف الأدوات التقنية لتحليل مجموعات أكبر من البيانات، يمكنهم أن يقوموا بالتحليل المتقدم عبر الزمان أو المكان أو اللغة. في ٢٠١٦، حللت أبودو، وهي سوق إسكانية على الإنترنت، ملايين التغريدات لترى تباين استخدام اللغة التحقيرية بشأن العِرق والإثنية والنوع الاجتماعي والدين والتوجه الجنسي فيما بين أنحاء عدة من الولايات المتحدة. في ٢٠١٤، أجرت الأصوات العالمية «تحليلًا عاطفيًا» لتغريدات روسية بشأن خطر الحرب في القرم، أظهر ضعف المعارضة.

بداية أبحاث وسائل التواصل الاجتماعي

استَخدِم دائمًا وسائل التواصل الاجتماعي للمناصرة الحقوقية وكسب التأييد بطريقة آمنة وأخلاقية ومؤثرة. ينبغي عليك أن تكتشف وتنظم وتحفظ وتتحقق. الأسئلة التالية الغرض منها توفير الإرشاد. استخدمها في بحثك بغض النظر عن المنصات التي تعمل عليها.

أي المنصات والتطبيقات يسود استخدامها في بلدك أو منطقتك؟

«وسائل التواصل الاجتماعي» تعبير عام، وتطبيقات المستخدمين تختلف عبر البلدان والمناطق. بينما يشتهر تويتر في الولايات المتحدة، قد يفضل الناس في مصر أو بوروندي استخدام الفيسبوك. التعرف على هذه الفروق أمر جوهري عند تتبع الأحداث المتعلقة بحقوق الإنسان.

ما الكلمات المفتاحية أو الهاشتاجات المستخدمة لمشاركة المحتوى الخاص بموضوعك؟

يتواصل الناس باستخدام كلمات مفتاحية أو هاشتاجات معينة. اتبع هذه الإرشادات لتكتشف المحتوى. مثال: استخدم رواد مواقع التواصل الاجتماعي في بوروندي #1212massacre (#مذبحة١٢١٢) لوصف أحداث العنف في ديسمبر/ كانون الأول ٢٠١٥. أيضًا، قد تكون اللغة التي يستخدمها الشهود أكثر انفعالية مما كنت تبحث عنه في البداية.

هل بإمكانك تضييق نطاق بحثك وفلترة النتائج؟

بعض منصات وسائل التواصل الاجتماعي تتيح البحث باستخدام الموقع أو التاريخ أو نوع المحتوى. على سبيل المثال، Tweetdeck (تويت دِك)، وهي أداة لإدارة تويتر، تمكنك من البحث عن الصور ومقاطع الفيديو وحسب، بينما تستبعد إعادات التغريدات. يمكنك أيضًا أن تنشئ قوائم بالمستخدمين ذوي الثقة لرصد المحتوى بشكل اختياري.

الصورة: تظهر أمثلة لنوعية الكلمات المستخدمة على وسائل التواصل الاجتماعي في حالات الأخبار العاجلة، متضمنة «أنا» و«الخاصة بي» التي قد تساعدك في البحث عن شهود العِيان. المصدر: دويتشه فيله/ مشروع ريفيل.

هل قمت بحفظ المحتوى الذي تراجعه؟

يمكن للمحتوى الإلكتروني أن يختفي بمنتهى السرعة. يمكن أن يزيله من رفعه أو الشبكة الاجتماعية المستضيفة له. احتفظ بلقطات من الشاشة للمنشورات أو قم بتحميل الصور. بالنسبة لمقاطع الفيديو، توجد أدوات مثل Video Vaulat(فيديو فولت).

هل بإمكانك التحقق من المعلومات؟

يجب التدقيق في رسائل وسائل التواصل الاجتماعي بحرص لتحري الدقة. قد يكون إغراء الاستخدام للمحتوى البصري الذي تتم مشاركته على نطاق واسع أكبر منه بالنسبة لشهادات شهود العِيان، ولكن لا بد من تطبيق نفس معايير التحقق.

هل لديك مصادر أخرى للمعلومات من أجل التأكيد؟

لا تعتمد على رسالة واحدة على وسائل التواصل الاجتماعي عندما تكون هناك على الأغلب منشورات ومقاطع فيديو وصور على الإنترنت تذكر نفس الواقعة. مزج أنواع المعلومات المختلفة بما تتضمنه من شهادات شهود العِيان والتقارير الإخبارية سوف يساعدك على بناء قضية أقوى بكثير.

هل ثمة مخاطر تتعلق بالخصوصية أو مخاوف أخلاقية؟

كما هو الحال مع أي مصدر، لا بد من النظر في أمر المخاطر المحتملة بالنسبة للأفراد عند مشاركة أو نشر كلماتهم أو صورهم. أيضًا، اسأل نفسك إذا ما كنت تضر بدون قصد بالمجتمعات الواقعة تحت وطأة النزاع.

في العمق

لا تلحق الضرر بأحد (لا ضرر ولا ضرار)

إن مبدأ «لا ضرر ولا ضرار» لهو إطار مفيد لا بد من وضعه نُصب أعيننا في سياق التحول السلمي للنزاعات (سواء كانت مسلحة أو غير ذلك). يملي علينا هذا المبدأ طرح الأسئلة حول ما إذا كانت التدخلات ستسهم في توحيد الصفوف أو في المزيد من الانقسام.

قد تُعمق مشاركة الصور المؤثرة أو مقاطع الفيديو لانتهاكات حقوق الإنسان أو للفظائع عبر وسائل التواصل الاجتماعي من هوة الانقسام بين طرفي النزاع، وفقًا لكيفية تقديمها. إذا ما انتشرت مواد مزورة تزعم إظهار فظائع، يمكن للصراع أن يزيد احتدامًا. وذلك يضعنا في مواجهة مخاوف أخلاقية شديدة الأهمية تتعلق بمشاركة محتوى وسائل التواصل الاجتماعي، كما يسلط الضوء على الأهمية القصوى للتحقق والتقديم المدروس للبيانات، بهدف إنهاء العنف وليس تأجيجه.

للحصول على المزيد من المعلومات بشأن مبدأ لا ضرر ولا ضرار (Do-No-Harm)، انظر:

Anderson, Mary B: "Do No Harm: How Aid Can Support Peace – Or War" Boulder, CO: Lynne Rienner Publishers, 1999.

الصورة: «اللاعنف»، صورة من الأمم المتحدة/ ميتشوس تزوفاراس (CC-BY-NC-ND 2.0)

ثلاث فئات من «التزييف» احذر منها على وسائل التواصل الاجتماعي

الإسناد المغلوط

تمثل هذه الفئة إلى حد بعيد أكثر التحديات شيوعًا في مجال أبحاث حقوق الإنسان. يُعاد تدوير المحتوى على الإنترنت بصفة مستمرة، وتتم مشاركته بتاريخ أو موقع أو إسناد مغلوط.

مثال

تمت مشاركة مقطع فيديو يحتوي على مشاهد شديدة القسوة أثناء أحداث عنف ما بعد الانتخابات في ساحل العاج في ٢٠١١. ولكن هذا المقطع كان يعود لعدة سنوات مضت. وجرت مشاركته في عدة بلدان بالفعل. وإحدى التقنيات البسيطة المستخدمة لاكتشاف المحتوى القديم هي القيام ببحث الصور العكسي. يمكن القيام بذلك أيضًا عن طريق صورة المعاينة الخاصة بالفيديو. (انظر فصل التحقق في هذا الدليل).

التلفيق

يمكن تلفيق مشهد أو واقعة أو تفاصيل معينة لحدث ما. على سبيل المثال، ظهرت جماعة مسلحة في سوريا في فيديو على اليوتيوب ومعهم ما تبين أنها ألعاب أطفال على شكل مسدسات.

مثال

كان «الطفل السوري البطل» مقطع فيديو ملفقًا، أنتجه أحد صناع الأفلام النرويجيين، وهو مثال كلاسيكي يُظهر أهمية طرح الأسئلة في أعقاب النظر إلى البصمة الأصلية والرقمية لرافع الفيديو. كانت قناة اليوتيوب التي استضافت الفيديو في بادئ الأمر جديدة واحتوت على هذا الفيديو شديد التأثير وحسب - جرس إنذار.

التلاعب التقني

كن على حذر من السهولة المتزايدة التي يمكن من خلالها التلاعب بالمحتوى، وبخاصة الصور، عن طريق القص أو محو التفاصيل أو دمج الصور لتحريف الأحداث.

مثال

في ٢٠١٣، نشر مسئولون من مقاطعة آنهوي بالصين صورة معالجة تظهر نائب العمدة «يُحلق كشبح فوق سيدة مُسنة بحجم دمية». بعد موجة من السخرية الإلكترونية، اعترفوا بأن الصورة كانت نتيجة لدمج صورتين، وعبروا عن «بالغ أسفهم».

البيانات التي ستصمد في المحكمة

الأدلة المقبولة قانونًا

لتوثيق حقوق الإنسان أثر قوي على الإجراءات القانونية. تسعى المحكمة الجنائية الدولية، كما العديد من المحاكم المختلطة، بشكل نشط إلى الحصول على دعم المجتمع المدني. ولكن المحاكم تتسم بالبطء فيما يتعلق بتبني التكنولوجيات الجديدة، والقضاة – وخاصة من هم أكبر سنًا – عادةً لا يكونون على دراية بكيفية تحويل البيانات الرقمية إلى قواعد إثباتية عادية. سيختلف الأمر ما بين دائرة قضائية والأخرى فيما يتعلق بقبول فيديو من يوتيوب كحجة قانونية من عدمه.

على سبيل المثال، في ٢٠١٥، حاكَم النظام القضائي السويدي مقاتلًا سابقًا من سوريا بتهمة التعذيب بناءً على فيديو نشر على فيسبوك. العديد من السوريين يقومون بالاضطلاع بمهمة جمع مثل هذا المحتوى الإلكتروني لأغراض الملاحقة القضائية بالخارج للمسئولين والعسكريين والمقاتلين السوريين السابقين الذين فروا خارج البلاد.

متطلبات المحكمة

إذا ما رغبتَ في أن تقود بياناتك إلى محاكمات جنائية، فلابد وأن تتأكد من تسجيل كل الميتاداتا ذات الصلة. لا بد وأن تتمكن المحكمة من التعرف بوضوح على موقع الفيديو إما من خلال إحداثيات الموقع المدمجة بالفيديو وإما من خلال المعالم التي يمكن التعرف عليها عبر محتوى الفيديو. وبالإضافة إلى ذلك، فإن مادة الفيديو لا بد وأن تكون واضحة – مقاطع الفيديو الغائمة أو المهتزة التي تلقي بالشكوك على هوية من يظهر بالفيديو أو ماهية ما يفعله غالبًا لن تُقبل.

أيضًا خذ في اعتبارك تسلسل الحيازة، من أجل قبول المحتوى في محاكمة جنائية، ستحتاج معظم المحاكم إلى معرفة كل فرد تداول المحتوى، بدءًا من المنشئ الأصلي ووصولًا إلى المُدعي الموجود في قاعة المحكمة. يجب أن يظهر تسلسل الحيازة بالضبط (من حاز المحتوى ومتى ولأي مدة من الوقت) من أجل المساعدة في الحماية من التلاعب بالأدلة. كلما اقتربت من الفيديو الأصلي، تيسر تقديمه في المحكمة؛ لأن تسلسل الحيازة يصبح أقصر وأسهل في العرض.

كما سيكون من الأهمية بمكان أن تعمل بشكل محايد وألا تعبث بالبيانات بقدر المستطاع. قد يحتج محامي الدفاع بفساد البيانات أو تحيزها أو احتوائها على دوافع غير لائقة. سوف تحتاج إلى إجراء شيء من التحليل على الأقل لتجعل توثيقك قابلاً للبحث ومفهومًا، ولكن حاول التقليل من عملية التحليل بقدر الإمكان.

مخاطر اللجوء للمحاكم

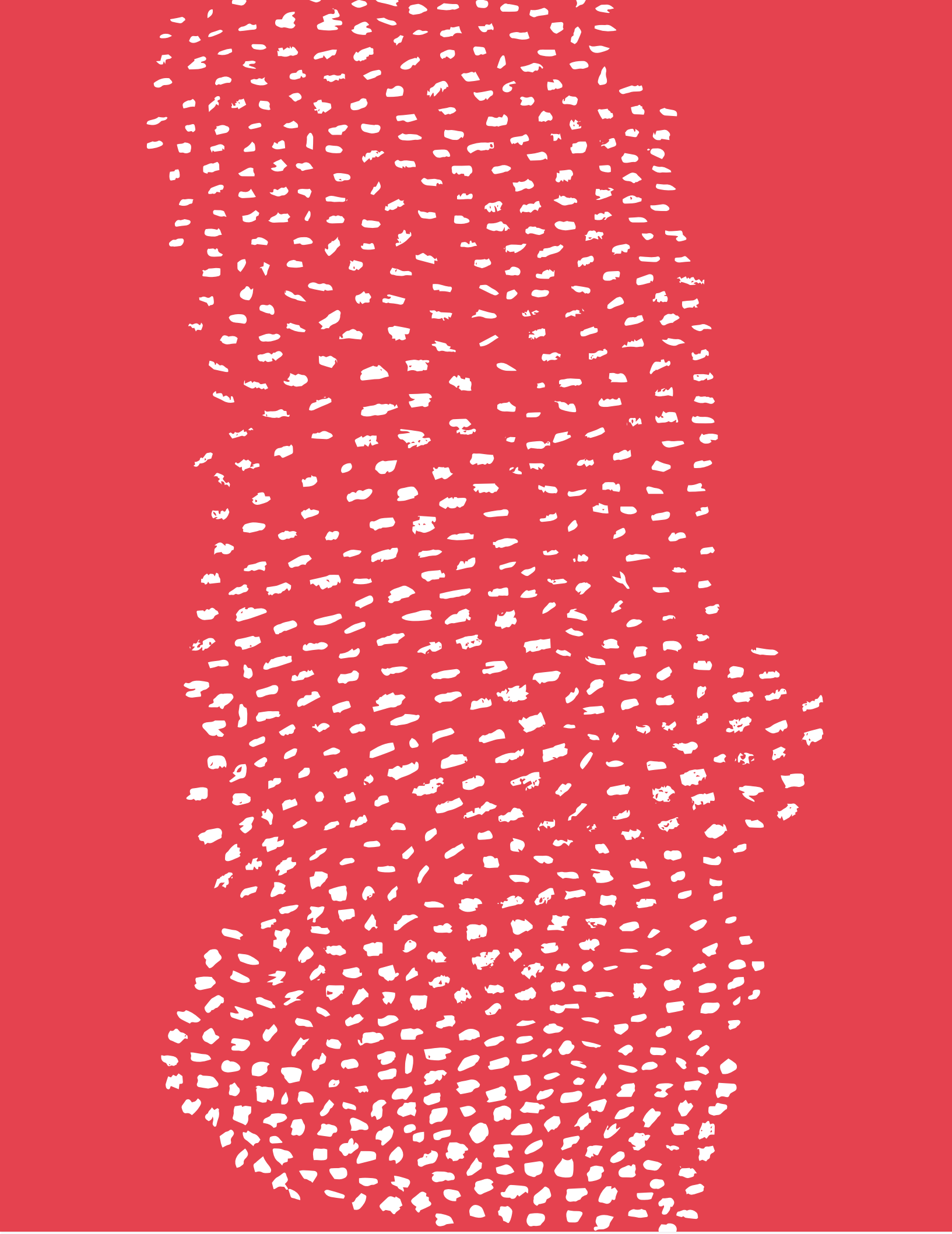
باللجوء للمحاكم، تتعرض منظمات حقوق الإنسان لمخاطرة الخضوع لمذكرة إحضار تحتم عليها الكشف عن أدلة سرية، مثل الأسماء والتواريخ، في محكمة علنية بسبب إجراء سابق على المحاكمة يتيح لكل طرف الاطلاع على أدلة الطرف الآخر.

إذا كنت تعمل مع ممثل الادعاء، حاول أن تصل معه إلى نظام لحماية الشهود. الكثير من إجراءات التقاضي علنية، ويمكن أن تذهب جميع احتياطاتك أدراج الرياح في التو واللحظة إذا أدلى الشاهد بشهادته وجرى الإفصاح عن اسمه ومعلوماته الشخصية. تجنب اللجوء إلى المحاكم التي لا تحمي الشهود حتى لا يضار شهودك كنتيجة لشهاداتهم.

أشكال أخرى من العدالة

وحتى لو كانت هذه المخاطر كثيرة ومحيرة، فما زال هناك بصيص من الأمل. المركز السوري للعدالة والمساءلة- وهو منظمة تعمل على جمع انتهاكات حقوق الإنسان والقانون الإنساني الدولي في النزاع السوري- قد جمع ما يزيد عن مليون وحدة من البيانات على مدار خمس سنوات. معظم التوثيق؛ ربما ما يربو على ٩٠ بالمائة، غالبًا ما لن يُقبل في المحكمة، ولكن جميع التوثيقات المتبقية يمكن استخدامها في أنواع أخرى من عمليات العدالة الانتقالية.

تتضمن العدالة الانتقالية لجان تقصي الحقائق وبرامج التعويضات والتأبين والإصلاح المؤسسي، والتي يمكنها جميعًا أن تساعد في التعافي وجبر أضرار الماضي والتحرك نحو المصالحة. في حالة الإصلاح المؤسسي، يمكن لمجموعات البيانات الكبيرة أن تُظهر النزعات المسيئة والفاسدة في القطاع القضائي لبلد ما. يمكن لهذه البيانات أن تساعد في عرض جوانب من القطاع تتطلب الإصلاح ويمكنها أن ترشد عملية التدقيق والإصلاح القضائي لبلد ما. عن طريق إصلاح قطاع العدالة، يمكن للبلد أن يمضي نحو ضمان عدم تكرار ما حدث سابقًا.



تقنيات عمليـة

إحصاءات الحكومة المفتوحة

تجمع الحكومات البيانات من أجل دعم عمليات اتخاذ القرار والتخطيط. هناك ضغط على الحكومات من أجل فتح بياناتها للجمهور لزيادة الشفافية والمساءلة وإشراك المواطنين. وتتزايد أمثلة مبادرات البيانات المفتوحة عالميًا، بما يشتمل على البوابات والتطبيقات الإلكترونية المتاحة للمواطنين للوصول إلى بيانات الحكومة ذات الصلة لاستخدامهم الخاص. يمكن لهذه المصادر أن توفر منجمًا من المعلومات ذات الصلة لباحثي حقوق الإنسان، ولكنها، في الوقت ذاته، قد تطرح تحديات.

الحصول على البيانات الحكومية

هناك كم كبير من البيانات الثانوية متاح للجمهور على المواقع الإلكترونية الخاصة بمكاتب ومراكز الإحصاء الوطنية. وبالإضافة إلى ذلك، تنشر العديد من الوكالات تقييمات للبرنامج الحكومي على الإنترنت.

عندما لا تكون البيانات متاحة على الإنترنت، قد يمكنك التقدم بطلب لحرية المعلومات. تعترف أكثر من ٩٥ بلد بالحق العام في الحصول على المعلومات الحكومية، مع استثناء المعلومات التي تملي حساسيتها عدم نشرها. اقرأ المزيد على: *http://right2info.org*

تحميل البيانات الحكومية وتخزينها وتنظيمها

عادةً ما تقدم البيانات الحكومية في صيغة بي دي إف، مما يصعب من عملية تحليل البيانات والبحث فيها. تُقدم مدرسة البيانات دورات تعليمية عن كيفية استخلاص البيانات من ملفات البي دي إف، حتى تتمكن من العمل بصيغة مألوفة وسهلة الاستخدام مثل السي إس في أو الإكس إل إس إكس.

أنواع البيانات الحكومية

نوع البيانات	أمثلة	المميزات	العيوب
السجلات الإدارية تنشأ عند تفاعل الوكالات والمؤسسات الحكومية مع الجمهور. يمكنها أيضًا أن تتضمن بيانات العمليات التجارية المعنية بموردي الخدمة والماليات.	الإحصاءات الحيوية المعنية بالسكان، مثل معدلات الوفيات والمواليد؛ وكذا إحصاءات العمالة والباحثين عن الوظائف. المنتفعين من السياسات والخدمات الاجتماعية. عقود البائعين ومسك الدفاتر.	عندما تُحدث السجلات الإدارية بشكل مستمر، يمكنها أن تمثل موردًا نوعيًّا بسيطا وسهل التتبع، بحيث يمكنه تحسين الشفافية واجتثاث الفساد من جذوره.	تُسجل فقط لمن يستخدمون خدمة عامة بعينها، لذا فلا يمكن الوثوق في التغطية على طول الخط. على سبيل المثال، قد تقلل إحصاءات الجريمة من تمثيل الاعتداءات الجنسية، لأن عدد البلاغات عن مثل هذه النوعية من الجرائم أقل بكثير من عدد الجرائم الفعلية.
المسوح الإحصائية تجمع المسوح الإحصائية – والتي تُسمى أيضًا بالمسوح بالعينة – البيانات من مجموعة جزئية من السكان وحسب، بهدف التوصل إلى استنباطات تنطبق على السكان ككل.	مسوح الصحة الديموغرافية ومسوح القوى العاملة ومسوح دخل الأسرة ونفقاتها.	يمكن للمسوح أن تمثل طريقة مجدية التكلفة بالنسبة للحكومات من أجل جمع المعلومات حيثما لا تتوافر البيانات من المصادر الإدارية.	قد يؤدي تحيز الاختيار إلى عدم تمثيل العينة المستخدمة لسائر السكان.
التعدادات السكانية فهرس يجمع كل أعضاء البلد أو المنطقة.	عادةً ما تُجري البلدان تعدادات للسكان والإسكان والزراعة والمنشآت الصناعية.	تُوفر التعدادات بيانات خط الأساس فيما يتعلق بالخصائص الرئيسية للسكان وكذا المتغيرات التي لا تتغير بسرعة.	عادةً ما يتم إجراء التعداد السكاني كل عشر سنوات نظرًا لتعقيد العملية وتكلفتها.

تقييم موثوقية البيانات الحكومية

بيانات الحكومة ليست دقيقة على الدوام. ليس من النادر أن تحتوي قواعد البيانات الحكومية وغير الحكومية على معلومات متضاربة. ومن الأسباب الرائدة لمثل ذلك التضارب: الطرق المختلفة لجمع البيانات والتحليل والحساب.

المفهوم	التعريف	المشكلات المحتملة
الصحة	لا بد أن تعكس البيانات ما تحاول قياسه (مثلًا: إعمال حق ما) بأكبر قدر ممكن من الدقة والمباشرة.	تُجمع معظم البيانات الثانوية لاستخدامات غير رصد حقوق الإنسان، وبالتالي فلا بد من إعادة توظيفها وتفسيرها في السياق الجديد. يمكن لعملية إعادة التفسير تلك أن تمثل تحديًا.
الموثوقية	تشير إلى اتساق البيانات أو إمكانية الاعتماد عليها؛ وذلك يعني أن البيانات المجموعة عدة مرات بنفس الطريقة لا بد وأن تنتج عنها نتائج مماثلة.	قد تؤدي الالتباسات أو التحيزات في طريقة جمع البيانات (مثلًا: كيفية تأطير أسئلة المسح أو كيفية أخذ عينات من السكان) إلى انعدام موثوقية البيانات.
الحيادية	لا بد وأن يتم جمع البيانات بطريقة تحترم الاستقلال العلمي وبأسلوب يتسم بالموضوعية والمهنية والشفافية.	قد يقوم مركز إحصائي وطني «بتعديل» الأرقام حتى يبدو موقف ما أفضل مما هو عليه فعليًّا.

من أجل تقييم صحة البيانات وموثوقيتها وحياديتها، اطرح الأسئلة التالية:

- **ما هو موضوع البيانات؟**

  فيما يتعلق ببعض الموضوعات الحساسة أو المثيرة للجدل، قد تشتهر البيانات الحكومية بانعدام موثوقيتها.

- **كيف يتم تأطير أسئلة المسوح؟**

  في بعض الأحيان تكون الأسئلة إيحائية، وبالتالي تتسبب في تحيز الإجابة.

- **ما هو حجم العينة؟**

  قد تكون أصغر من أن تعتبر ممثلة.

- **ما هي الفترات التي تجمع على مدارها البيانات؟**

  قد تكون البيانات متقادمة.

- **من يجمع البيانات؟**

  احتمالية تضارب المصالح أو محدودية الموارد.

- **من ينشر البيانات؟**

  احتمالية تضارب المصالح.

تحليل البيانات من منظور حقوقي

عند دمج البيانات الحكومية وتحليلها على أساس معايير ومبادئ حقوق الإنسان، يمكن للبيانات الحكومية أن تفيد في كشف انتهاكات الحقوق الاقتصادية والاجتماعية والثقافية. لذا، فإنه من المفيد عند النظر إلى الإحصاءات الحكومية أن نطرح السؤال التالي: ما الذي يخبرني ذلك به بشأن إتاحة السلع والخدمات وإمكانية الحصول عليها وجودتها؟ هل ثمة مناطق بعينها أو مجموعات معينة تعاني من التهميش أو التمييز؟ كيف تغيرت الأمور بمرور الوقت؟ هل تحسنت أم ساءت؟

دراسة الحالة

البيانات الحكومية بوصفها دليلاً على التمييز المنهجي في جواتيمالا

في ٢٠٠٩، نشر كل من مركز الحقوق الاقتصادية والاجتماعية ومعهد أمريكا الوسطى للدراسات المالية تقريرًا بشأن الحق في الرعاية الصحية للأمهات في جواتيمالا، أظهر أدلة على التمييز ضد النساء من السكان الأصليين.

اعتمادًا على البيانات الصادرة عن البنك الدولي وبرنامج الأمم المتحدة الإنمائي ومكاتب الإحصاء الوطنية، أوردت الجهتان المذكورتان عاليه مسوح الصحة الديموغرافية التي تظهر أن نتائج جواتيمالا فيما يتعلق بوفيات الأمهات هي من ضمن الأسوأ والأقل إنصافًا في أمريكا اللاتينية؛ حيث تضاعفت احتماليات وفاة النساء من السكان الأصليين أثناء الحمل أو الولادة ثلاث مرات بالمقارنة بنظيراتهن من السكان غير الأصليين، وكان بالإمكان منع ٥٠٪ من الوفيات عن طريق العناية المتخصصة. كما أظهرت الإحصاءات الإدارية مشكلات جمة فيما يتعلق بإتاحة الخدمات وجودتها.

ارتبط التنفيذ الرديء للسياسات باستثمار الموارد الهزيلة في قطاع الصحة. ظلت مخصصات الصحة تمثل حوالي ١٪ من إجمالي الناتج المحلي منذ نهاية الحرب في ١٩٩٦، وذلك أدنى من مثيلاتها في دول أمريكا الوسطى الأكثر فقرًا. كما اتسم توزيع نصيب الفرد من الإنفاق على قطاع الصحة بالظلم الشديد؛ حيث وجهت ثلاثة أضعاف النقود الموجهة إلى كيتشيه – أفقر مناطق جواتيمالا – إلى العاصمة. اقترن الإنفاق الاجتماعي المتدني مباشرة بقاعدة ضرائب البلد المنخفضة، والتي كانت في معظمها تتولد من الضرائب التنازلية غير المباشرة، والتي تستهدف الفقراء بشكل غير متناسب، في الوقت ذاته الذي تتمتع فيه قطاعات الأعمال في البلد بالمحفزات والامتيازات الضريبية.

اجتمعت كل هذه الأرقام لتبني الاستنتاج القوي بأن جواتيمالا لم تكن تفعل كل ما بوسعها لتحسين صحة الأمهات، مما أدى على أرض الواقع إلى التمييز ضد النساء الأكثر فقرًا من السكان الأصليين. انظر التقرير كاملًا هنا: http://www.cesr.org/section.php?id=33

الصورة: منظر لشارع، تشاهول، كيتشيه في جواتيمالا (٢٠١٤) لآدم جونز على فليكر (CC-BY-SA 2.0).

تقنيات عمليـة

بيانات الموازنات لحقوق الإنسان

عند وضع أولويات الموازنة، يمكن للحكومات أن تتغاضى عن معايير حقوق الإنسان، بقصد أو بغير قصد. على سبيل المثال: قد تؤدي تخفيضات الموازنة في نظام العدالة الجنائية إلى ترك المتهمين ذوي الدخول المنخفضة في الحبس الاحتياطي لفترات طويلة للغاية. قد يمثل القرار بتخفيض الدعم أو زيادة الضرائب على أسر بعينها أو منتجات صحية معينة تمييزًا غير مباشر ضد المرأة. لذا، فإن الإلمام ببيانات الموازنة يمكنه أن يمثل مكونًا أساسيًّا للعمل البحثي الشامل في مجال حقوق الإنسان، خاصة مع إتاحة الكثير والكثير من البيانات على الإنترنت حاليًّا.

أنواع البيانات الموازنية

قد يفيدنا تقسيم الموازنة إلى ثلاثة أجزاء رئيسية: كيفية توليد العوائد، وكيفية تخصيص الموازنات، وكيفية الإنفاق فعليًّا.

بيانات عوائد الموازنة

هل تولد السياسات الضريبية ما يكفي من الموارد؟ هل يتم ذلك بصورة تتسم بالإنصاف؟

تتضمن البيانات المفيدة للحكم على كفاية الموارد ما يلي:

- العائد الحكومي في صورة نسبة مئوية من إجمالي الناتج المحلي.
- العائد الضريبي في صورة نسبة مئوية من العائد الحكومي
- الجهد الضريبي (نسبة تحصيل الضرائب الفعلية إلى السعة الضريبية).
- حجم التدفقات المالية غير المشروعة.
- العائد الضريبي في صورة نسبة مئوية من إجمالي العائد الضريبي.

تتضمن البيانات المفيدة للحكم على إنصاف الموارد فما يلي:

- تكوين الضرائب (مثلًا: نسبة مئوية تتكون من ضريبة الدخل، الضرائب على السلع والخدمات، ضريبة الشركات، إلخ...).
- الضريبة في صورة نسبة مئوية لإجمالي الدخل المدفوع من قِبل مجموعات مختلفة.
- الإعفاءات الممنوحة.

دراسة الحالة

الأموال المتسربة

يخصص بلد ما ١,٥٪ من موازنته لقطاع الصرف الصحي. انخفض هذا المخصص على مدار السنوات العشر الماضية. ٧٥٪ من الأموال المخصصة للصرف الصحي تصب في دعم الصرف الصحي المائي (أي مواسير المجاري)، ولكن الأسر الفقيرة في الأحياء العشوائية تعتمد على الصرف الصحي الموضعي (مثل الحفر المرحاضية). هل يُعد ذلك جرس إنذار من منظور حقوقي؟ قد تكون الحكومة، بشكل فعلي، تمارس التمييز ضد الأسر في الأحياء العشوائية.

تتيح شراكة الموازنة الدولية سلسلة من الموارد التي تشرح كيف يمكن لمعايير حقوق الإنسان الدولية مثل الإعمال التدريجي وعدم التمييز والحد الأقصى من الموارد المتاحة المساعدة في الإجابة عن هذا السؤال:
http://www.internationalbudget.org/publications/escrarticle2/.

في العمق

ما هي الميزنة المراعية للمنظور الجنساني؟

الميزنة المراعية للمنظور الجنساني هي نوع معين من أنواع تحليل الموازنات، يُستخدم لتقييم أثر العائد والإنفاق الحكوميَّين على النساء والرجال والفتيات والفتيان. على سبيل المثال، في مجال الصحة: للرجال والنساء احتياجات متماثلة فيما يتعلق بالإنفلونزا والملاريا، ولكن من ناحية أخرى، تزيد احتياجات النساء عن الرجال فيما يتعلق بالصحة الإنجابية. تمثل الميزنة المراعية للمنظور الجنساني طريقة جديدة ومتطورة لتصور الآثار التمييزية للقرارات المتعلقة بالموارد ومعالجتها. توجد موارد مفيدة بشأن هذا الأمر على www.gender-budgets.org.

الصورة: وحدة سان مالِن للصحة الأولية ببوجِن، منطقة بو، سيراليون . الصورة على فليكر لـ « H6 Partners »CC-BY-NC-ND 2.0

بيانات تخصيص الموازنة

يمكن للخطوات التالية أن تحدد إذا ما كانت تخصيصات الموازنة متوافقة مع معايير ومبادئ حقوق الإنسان.

١. **الحساب:**
- النسب أو الحصص (النسبة المئوية لشيء ما من الإجمالي).
- المتوسط (القيمة المتوسطة لمخصصات الموازنة).
- إنفاق الوحدة أو الفرد (القيمة لكل شخص).

٢. **عقد المقارنات**
- التعرف على المجالات والمجموعات ذات الأولوية.

٣. **تحليل الاتجاهات** (مقارنة التقدم على مدار الوقت، مع تعديله وفقًا للتضخم).

البيانات المعنية بإنفاق الموازنة

عادةً ما يختلف تخطيط الحكومة بالنسبة للإنفاق عن إنفاقها الفعلي. الفساد سبب رئيسي، ولكن يمكن لكل من نظم الإدارة المالية غير الكُفء وتحويل مسار الأموال والإشراف الضعيف أن تسهم في توسيع الهوة.

توجد مجموعة متنوعة من الأدوات والطرق (عادةً ما يطلق عليها مقاربات «اتبع الأموال») التي تتابع البيانات المتعلقة بالإنفاق، بما يتضمن: تقارير الرقابة والإشراف الحكومية ورصد عملية التوريد العامة والرقابة والإشراف غير الحكوميين على الإنفاق.

الوصول إلى البيانات الموازنية

الموازنات هي مستندات حكومية رسمية. بشكل عام، يجب أن تكون متاحة على المواقع الإلكترونية لوزارة الخزانة أو المالية، أو مكاتب الرقابة العامة أو وكالات مكافحة الفساد. ولكن في بلدان عدة، لا يتم الإعلان عن المستندات ذات الصلة، ولا توفر إلا قلة قليلة من الحكومات الآليات المناسبة لمشاركة الجمهور في عمليات الموازنة.

لمعرفة مدى انفتاح عملية الموازنة لدى حكومتك، قم بزيارة **مؤشر الموازنة المفتوحة**، والذي يرتب الدول وفقًا لدرجة تمكن الجمهور من الوصول إلى ثمانية مستندات رئيسية في عملية الموازنة.

تتوفر مصادر أخرى للبيانات ذات الصلة بتحليل الموازنات من المؤسسات المالية الدولية، مثل البنك الدولي وصندوق النقد الدولي. يمكن للمنظمات غير الحكومية التي تعمل في مجال الفساد أن تساعدك أيضًا في تحديد البيانات الموازنية.

وفقًا لمنطقتك والسياق السياسي، قد يكون من الحكمة استخدام VPN (شبكة افتراضية خاصة) أو أي من أدوات التخفي الأخرى لحجب عمليات بحثك عن بيانات الموازنة.

بداية دراسة الحالة

تخفيضات الموازنة التمييزية في إسبانيا

حللت دراسة أجراها مركز الحقوق الاقتصادية والاجتماعية في ٢٠١٢ سياسات التقشف الإسبانية من منظور حقوقي. أظهرت بيانات الدخل أن ربع السكان وما يقرب من ثلث الأطفال جميعًا يواجهون خطر الفقر والاستبعاد الاجتماعي. كما كانت هناك فروق شاسعة بين المناطق المختلفة.

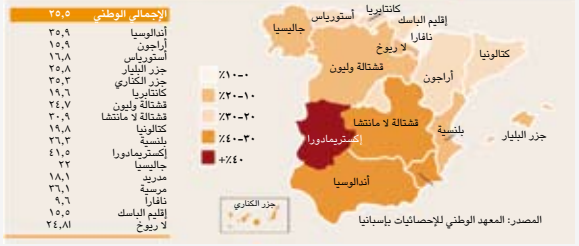
في مايو/ أيار ٢٠١٢، صادقت إسبانيا على أكبر استقطاعات موازنية على مر تاريخها الديمقراطي، بما يصل إلى ٢٧,٣ مليار يورو. كان المبرر هو تقليص العجز العام. ولكن الخبراء حذروا من أن هذه الاستقطاعات سوف تكون على حساب إتاحة الخدمات الاجتماعية الأساسية واستدامتها.

وفقًا لفكرة خاطئة منتشرة، كان هناك اعتقاد بأن الأزمة المالية في إسبانيا سببها التجاوز في الإنفاق. في حقيقة الأمر، كانت إسبانيا من ضمن أقل الدول إنفاقًا على الحماية الاجتماعية والصحة والتعليم في أوروبا.

كان لإسبانيا اقتصاد ظل ضخم، مما تسبب في خسارة كبيرة للعائد. أَجرى الاتحاد الإسباني لمفتشي الضرائب حساباتهم التي أظهرت أنه إذا ما تمكنت إسبانيا من التحكم في حجم اقتصاد الظل لديها بحيث يصبح متسقًا مع معايير الاتحاد الأوروبي، فإنها ستتمكن من توليد ٣٨ مليار يورو، بما يزيد عن إجمالي تخفيضات الموازنة لعام ٢٠١٢.

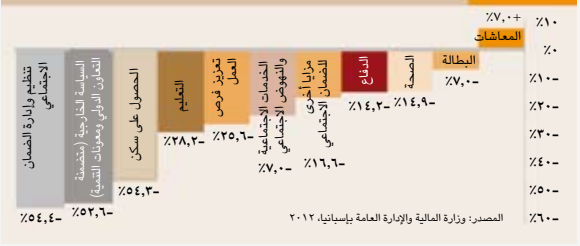
استنتج الباحثون أنه بالتركيز حصريًا على تخفيضات الإنفاق العام، يُحرم الناس من حقوقهم الاجتماعية والاقتصادية الأساسية. وبدون النظر في البدائل لتقليص العجز، أخفقت إسبانيا في الوفاء بالتزاماتها المنصوص عليها في العهد الخاص بالحقوق الاقتصادية والاجتماعية والثقافية.

شكل ١١ النسبة المئوية للسكان المعرضين لخطر الفقر أو الاستبعاد الاجتماعي على يد المناطق المتمتعة بالحكم الذاتي في إسبانيا (٢٠١٠)



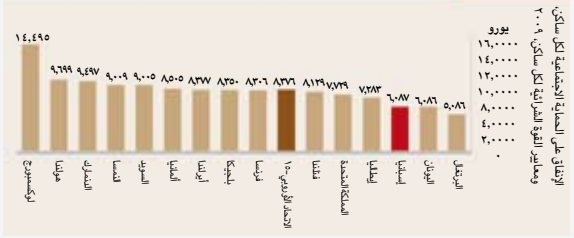
المصدر: المعهد الوطني للإحصائيات بإسبانيا

شكل ١٤ استقطاعات الموازنة الوطنية من القطاع الاجتماعي وقطاعات أخرى: النسبة المئوية للتغيير من ٢٠١٠ - ٢٠١٢

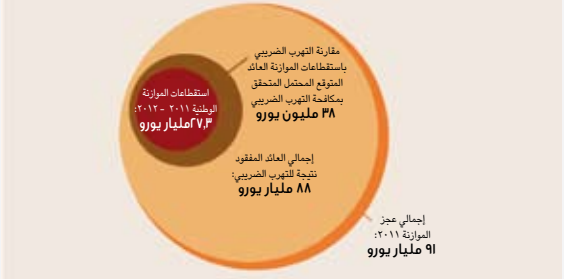


المصدر: وزارة المالية والإدارة العامة بإسبانيا، ٢٠١٢

شكل ١٥ الإنفاق السنوي على الحماية الاجتماعية والصحة والتعليم للفرد في الاتحاد الأوروبي - ١٥ (أحدث الأرقام المتاحة)



شكل ١٩ التهرب الضريبي واستقطاعات الموازنة في اسبانيا (٢٠١٢)



المصدر: وزارة المالية والإدارة العامة بإسبانيا، ٢٠١٢ ومصلحة الضرائب الإسبانية حستا، ٢٠١١

موجود اليوم، مختفٍ غدًا: الحفاظ على مقاطع الفيديو والصور على الإنترنت

تخيل أنك وجدت فيديو على الإنترنت يفضح انتهاكًا وتحققت منه، ولهذا المقطع القدرة على تقوية قضية أو حملة مناصرة تعمل عليها، لذا تقوم بحفظ الرابط. بعد عدة أيام، يختفي المقطع...

ممكن لمقاطع الفيديو والصور على الإنترنت أن تختفي بسرعة، بخاصة إذا ما كانت تحتوي على مشاهد عنيفة أو تتعلق بقضايا حقوق الإنسان الحساسة. من يناير/ كانون الثاني إلى يونيو/ حزيران ٢٠١٥، أزال يوتيوب ما يزيد عن ٥٧٠٠ فيديو استجابة لمطالب الحكومات فقط. ولذلك السبب ينبغي عليك ألا تعامل منصات الإنترنت بوصفها وحدات تخزين للبيانات. قد يتم مسح مقاطع الفيديو من قبل من رفعها أو المنصة لعدة أسباب، منها مخالفة شروط الخدمة أو شكاوى المستخدمين أو التعدي على حقوق النشر أو إلغاء الحساب، أو إذا ما أغلقت المنصة بأكملها.

يكفل الاحتفاظ بالمحتوى الإلكتروني مثل الصور ومقاطع الفيديو وما تشتمل عليه من ميتاداتا لك إمكانية الوصول إليه في المستقبل، كما أنه سيساعدك على الحفاظ على مصداقية البحث، ويمكنك من فهرسة البيانات، ويؤسس لتسلسل الحيازة الذي قد تحتاج إليه في السياقات القانونية.

كيفية التحميل

إذا ما أجريت بحثًا على محرك بحث جوجل باستخدام كلمات «تحميل فيديو من يوتيوب»، ستجد عدة أدوات مجانية مثل Video Vault لحفظ الصور ومقاطع الفيديو الإلكترونية. كما توجد أيضًا مكونات إضافية للمتصفحات ونصوص مخصصة متاحة لتحميل كميات كبيرة من المحتوى. انتبه إلى أن حفظ المحتوى الإلكتروني يخالف بنود وشروط العديد من المواقع. من الأهمية بمكان أن تكون مسئولًا فيما يتعلق بالمحتوى الذي تحفظه وتشاركه، وأن تنسبه إلى المنشئ أو الرافع الأصلي.

احذر: يمكن أن تكون هناك برمجيات خبيثة بداخل برامج تحميل المحتوى، يمكنها عند التحميل أن تتسبب في الإضرار ببياناتك وخصوصيتك. ابحث عن البرمجيات مفتوحة المصدر الحاصلة على تقييمات جيدة، وقم دائمًا بتحميل البرمجيات مباشرة من موقع المطور أو من مصدر موثوق.

أنشطتك على الإنترنت ليست مُجهَّلة. لتجنب المراقبة التي تستهدف العمل في مجال حقوق الإنسان، انظر في استخدام شبكة افتراضية خاصة عند بحثك عن المواد الحساسة وتحميلك لها.

خطوات الحفظ الأساسية

١. حدد أي محتوى هو الأكثر صلة بمشروعك.

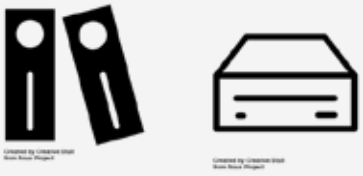
وأي ملفات ترغب في الاحتفاظ بها. حاول تحميل الملف بأكبر حجم ممكن واحفظ الملفات بصيغها الأصلية.

٢. استخدم طريقة متسقة في تنظيم الصور ومقاطع الفيديو.

على سبيل المثال، قم بتسمية المجلد وفقًا للسنة والشهر واليوم: ٢٠١٦/٣/١٦ بداخل المجلد، سمِّ الملفات بحيث تترتب تسلسليًا: 00001.AVI، ثم 00002.AVI ، إلخ...

٣. استخدم ملفًا نصيًا لتوثيق الميتاداتا.

لو كان المحتوى عنيفًا أو قاسيًا، وضح ذلك لتحذير المشاهدين. يجب أن يُخزن المستند النصي بجانب ملف صورة الفيديو. إذا ما كنت تجمع كمًا كبيرًا من المحتوى، فكر في إمكانية إنشاء فهرس.



٤. خزن المحتوى في مكان آمن، مثل بيت حليف تثق به

أو في خزانة في مكتب إحدى المنظمات غير الحكومية المعروفة، وقم بعمل نسختين احتياطيتين منه على قرصين أو جهازين منفصلين يُحفظان في مكانين مختلفين. انظر في استخدام التخزين السحابي الذي يركز بشكل صريح على التخزين الآمن للبيانات، مثل SpiderOak أو TeamDrive.

٥. تحقق من ملفاتك وأقراص التخزين خاصتك بشكل دوري.

للحصول على دلائل مفصلة بشأن هذه الخطوات، تفضل بزيارة archiveguide.witness.org

التقاط البث الحي

يمكن للبث الحي أن يوفر دليلًا ممتازًا غير معالَج، طالما تتم أرشفته بشكل ما أثناء البث نفسه. العديد من المنصات تقوم أوتوماتيكيًّا بأرشفة البث الحي، إذا لم ينطبق ذلك الأمر عليك، فينبغي أن تستبق تلك الحاجة بأن يكون لديك برنامج مثبت على جهازك لالتقاط هذا البث.

الشبكة الافتراضية الخاصة (VPN)، هي تكنولوجيا تنشئ اتصالاً آمنا على شبكة عامة مثل الإنترنت. يمكن لاستخدام برامج البروكسي على الشبكات الافتراضية الخاصة أن يساعدك على الاحتيال على فلترة الإنترنت. يمكنك الحصول على مزيد من المعلومات بشأن الشبكات الافتراضية الخاصة وبرامج البروكسي على دليل عدة الأمان الذي يقدمه كل من تكتيكال تيكنولوجي كوليكتيف، وفرونت لاين ديفندرز.

تنظيم فهرس للصور ومقاطع الفيديو

عند العمل مع كميات كبيرة من مقاطع الفيديو أو الصور، من الضروري استخدام الميتاداتا من أجل الفهرسة الفعالة. سوف يمكن هذا الأمر الباحثين من التعرف السريع على الملفات الصحيحة وتوفير الوقت الثمين.

ما الذي يدخل في المجموعة؟

قبل بناء الفهرس، سيفيدك التعرف على النتائج والأهداف والاستخدامات المرغوبة للفهرس. سيساعد ذلك على ضمان وثاقة صلة المحتوى الذي تجمعه بموضوعك.

» **لماذا يوجد الفهرس؟ ما الأهداف التي يخدمها الفهرس؟**
مثلًا: المناصرة وكسب التأييد، قضية قانونية، تقرير إعلامي، التوعية الجماهيرية، التأريخ لحادثة بعينها أو انتهاكات منتشرة، إلخ...

» **ما هو نطاق الفهرس؟**

» ما هي مقاطع الفيديو أو الصور التي ستقبلها؟ ما الذي لن تقبله؟

» كيف ستُنقل البيانات إليك؟

» ما هي المصادر أو الصيغ التي ستجمعها؟ شهود العِيان، مصادر مجهولة، أخبار/ وسائط إعلامية، بَث حي، إلخ...؟

» **ما هي المخاطر التي أنت على استعداد لمواجهتها؟**
مشاهد مصورة قد تعرضك أنت أو آخرين للخطر أو الاستدعاء للمثول أمام القضاء؟

» **هل يجب على بياناتك أن تكون قابلة للتشغيل على نظم آخرين غيرك؟**

الإتاحة: تعرف على مستخدميك ومساهميك

إن فهم مَن سوف يستخدم ويسهم في الفهرس سوف يساعدك على اتخاذ قرارات الإتاحة والإذن. عند النظر في الأمور الأمنيَّة، تعرف على المخاطر التي قد تواجهك لو أُتيح الفهرس للجمهور علنيًّا أو تم تخزينه على منصة غير مؤمَّنة.

» **مَن المستخدمون؟** حدد من يتاح له الوصول إلى محتواك.

» **كيف ستتعامل مع مسألة حقوق الاستخدام؟** مثلًا: المشاع الإبداعي، النسبة لفرد أو لمنظمة؟

» **هل سيكون الفهرس علنيًّا أم خاصًّا؟**
ما هي سياسات الإتاحة؟

» **مَن هم المساهمون؟** ما هو مدى إلمامهم بالتكنولوجيا؟ ما اللغات التي يتحدثونها؟ ما هي صيغ الملفات التي يستخدمونها؟

أسّس لسير العمل واختر منصة

- **ما هو سير العمل الذي ستوظفه لاستيعاب المحتوى والتحقق منه وفهرسته؟**
  مثلًا: تقارير شهود العِيان، استمارة إلكترونية، جدول بياناَت إلكتروني، في صورة مطبوعة، إلخ...
- **ما هي المنصات التي تفي بمتطلبات هيكل البيانات الخاص بك؟**
- **ما هي المعوقات التكنولوجية لديك؟**
  مثلًا: لا يوجد إنترنت، التمويل المحدود، لا توجد خبرة فنية، إلخ...
- **هل تتواءم المنصة وبيئتك الحوسبية؟**
- **ما اللغات التي يجب أن تدعمها؟**
- **ما هي المخاطر الأمنية الجوهرية للمنصة؟** هل تتوافق ومتطلبات أمنك؟
- **أي المنصات توفر أفضل سبل الأمن لبياناتك؟** فكر في الأمن في إطار نقل البيانات (المعلومات المتحركة) وفي إطار تخزينها (المعلومات الساكنة).
- **كيف ستشارك المعلومات مع مستخدمك النهائي؟**

في العمق

أمثلة على الأرشيفات الإلكترونية

بدأ الأرشيف الشيشاني في جمع ملفات الصور والفيديو والصوت من حرب الشيشان بدءًا من ١٩٩٤. من أجل تيسير مهمة العثور على معلومات الملفات واستخدامها وتصورها، قاموا بإنشاء فهرس شامل لتسجيل الميتاداتا الخاصة بكل ملف.

أرشيف الشعب لعنف الشرطة هو «أرشيف إلكتروني للقصص والذكريات والروايات المتعلقة بعنف الشرطة كما يتعرض لها ويسردها مواطنو كليفلاند، أوهايو». اطلع على شروط الخدمة للمساهمين للحصول على تفاصيل بشأن المحتوى الذي يقبلونه.

الأرشيف السوري هو أرشيف إلكتروني يحفظ مقاطع الفيديو التي توثق انتهاكات حقوق الإنسان وجرائم الحرب المرتكبة من قِبل جميع الأطراف أثناء النزاع السوري الدائر. بالإضافة إلى بناء قاعدة البيانات الإلكترونية، فإنهم يدعمون مؤيدي حقوق الإنسان في جهودهم التوثيقية.

هيكلة الفهرس

يساعدك التعاون مع المستخدمين النهائيين على التعرف على الهيكل الأمثل لفهرسك. على سبيل المثال، قد يخبرك محامي حقوقي أنه يحتاج الميتاداتا التالية: تاريخ وموقع حدوث جريمة مسجلة ونوع الجريمة وهوية الضابط ومعلومات الاتصال الخاصة بمصور الفيديو، ولكن بالنسبة لمن يعمل في مجال المناصرة وكسب التأييد، ربما يحتاج إلى معرفة اسم الضحية أو أين نُشر الفيديو للمرة الأولى.

- **ما هي المعلومات التي يحتاجها كل نوع من المستخدمين النهائيين من أجل الاستغلال الأمثل للمجموعة؟**
  انظر في إشراك المستخدمين النهائيين في عملية التطوير.
- **ما هو الحد الأدنى للميتاداتا المتاحة؟**
  ما هي العناصر اللازمة، وما التي يوصى بوجودها، وما هي العناصر الاختيارية؟
- **كم من الوقت يتوفر لديك من أجل الفهرسة؟**
- **هل تحتاج إلى حفظ تسلسل الحيازة وفهرسته لاحتمالية استخدام توثيقك للتقاضي الجنائي في المستقبل؟**
- **ما هي المعلومات التي يجب عدم الإفصاح عنها لأسباب أمنية؟**

الاستبقاء: التخطيط لعمر تخزيني واقعي لفهرسك

تمكنك معرفة فترة الاستخدام المتوقعة لفهرسك من أن تخطط لمشروعك بصورة أفضل، وتخصص الموارد وتُعرف نجاح المشروع.

- **إلى متى ستحتفظ بالفهرس؟**
  هل ستحتفظ بأنواع معينة من المحتوى لفترة أطول من أنواع أخرى؟
- **ما الذي سيحدث للفهرس؟** حدد خطة التداول: التخلص المسئول من البيانات وتسليمها، إلخ...
- **هل سياسة الاستبقاء لديك واقعية؟**
  مثال: هل بإمكانك الاحتفاظ بما تخطط له طوال المدة التي تخطط لها؟ هل ستكون قد عينت موظفين للحفاظ على المحتوى وتحديثه ورصده طوال عمر المجموعة؟

أمثلة للمنصات

- جداول بيانات جوجل/ نماذج جوجل
- جداول الإكسل الإلكترونية
- Filemaker Pro فيلم ميكر برو
- Martus مارتوس
- Omeka أوميكا
- Corroborator كوروبوريتُر

دراسة الحالة

استخدام الفيديو لفضح أنماط الانتهاك خلال الإخلاءات القسرية في البرازيل

في ٢٠١٢، تعاونت منظمة ويتنس مع ناشطين ومحامين وباحثين لتوثيق حالات الإخلاء القسري في ريو دي جانيرو وإبرازها ولمجابهة ادعاءات الحكومة بعدم حدوث أي انتهاكات سواء قبل أو أثناء أو بعد عمليات الإخلاء القسري المرتبطة بأعمال البناء الخاصة بكأس العالم ٢٠١٤ وأوليمبياد ٢٠١٦. استخدموا نماذج جوجل لجمع ما يزيد عن ١٠٠ فيديو من يوتيوب ومصادر شهود العِيان وتقارير الناشطين والإعلام وفهرستها وتصنيفها ووضعها في السياق الصحيح. استُخدمت البيانات لصياغة تقرير بشأن أثر عمليات الإخلاء واسعة النطاق.

الرسم بياني للبيانات يمثل أنواع الانتهاكات التي حدثت أثناء عمليات الإخلاء.

يوفر معمل ويتنس الإعلامي أمثلة وأفكارًا تتعلق بكيفية تصور فهرسك.

الصورة: الكفاح من أجل العدالة في البرازيل مظاهرة مناهضة للإخلاء في ماوا بالبرازيل ٢٠١٣، مكتبة صور CAFOD على فليكر CC-BY-NC-ND 2.0
https://www.youtube.com/watch?v=2eAIKhFj0m4

دليل الناشط لأرشفة مقاطع الفيديو

نظرة من أعلى: الأقمار الصناعية والطائرات بدون طيار

بينما يتزايد استخدام منصات المعلومات الجوية وتلك المعتمدة على الأقمار الصناعية في قطاعات تتراوح من الجراحة والزراعة إلى تخطيط المدن والمعونة الإنسانية، تتزايد أيضًا إتاحة المعلومات المجموعة من أجل إعادة استخدامها في أبحاث حقوق الإنسان أيضًا.

الصور الجوية والطائرات بدون طيار

على الرغم من أن الطائرات أو العربات الجوية بدون طيار قد تبدو وكأنها أشياء مستقبلية، إلا أنها ببساطة تعد طريقة لالتقاط المناظر من الجو، وهي بالفعل منتشرة الاستخدام في أوساط الهواة والمحترفين.

توفر المناظر الجوية تغطية شاملة للأرض، مما يفيد في بحث وتوثيق البنية التحتية والتغيرات البيئية والأضرار المترتبة على النزاع أو الكوارث الطبيعية وغير ذلك الكثير.

إذا ما رغبت في إطلاق طائرة بدون طيار تخصك، توجد موارد مفيدة متاحة من أجل البدء، والتجهيز للاستخدام، ولفهم الضوابط الوطنية والمحلية (تأكد من معرفتك بالقواعد وإلا فستُخاطر بتعرضك للتغريم أو مصادرة المعدات أو حتى إلقاء القبض عليك!)

الصورة: الجزيرة بلَس تشارك مقطع فيديو التقطته طائرة بدون طيار تحلق فوق حلب بسوريا في ٢٠١٥ لتظهر بوضوح مدى الدمار الذي أصاب المدينة جراء أربع سنوات من الحرب.]

عادةً ما يستخدم محققو حقوق الإنسان تصوير الطائرات بدون طيار الموجودة على منصات الإنترنت مثل Open Aerial Map (الخارطة الجوية المفتوحة أوبن آريال ماب) أو UAViators (يوآفياتُرز). ويتطلب هذا النوع من التصوير، والذي يرفعه إما الأفراد وإما المنظمات، سواءً كانوا معروفين أو مجهولين، نفس خطوات التحقق اللازمة لأي نوع آخر من المحتوى الإلكتروني.

الأقمار الصناعية لحقوق الإنسان

في يناير/ كانون الثاني ٢٠١٥، نشرت النيويورك تايمز قصة الغلاف عن هجوم بوكو حرام على بلدتين في شمالي شرق نيجيريا. من أجل إظهار حجم الدمار الشاسع على البيوت، استخدموا صور الأقمار الصناعية التي وفرتها العفو الدولية وهيومان رايتس واتش، ويُعد ذلك مثالا قويًّا على قدرة التصوير بالأقمار الصناعية على توطيد أبحاث حقوق الإنسان ومناصرتها.

لم تعد صور الأقمار الصناعية حِكرًا على الحكومات، وستتيح الاتجاهات الجديدة في توريد الصور هذا النوع من البيانات أكثر فأكثر في المستقبل. وكل من المجموعات الصغيرة والكبيرة قادرة بالفعل الآن على استخدام صور الأقمار الصناعية لعمل حقوق الإنسان اليومي.

مزايا صور الأقمار الصناعية:

» **الوصول المادي:**
تتيح الأقمار الصناعية التحايل على القيود المفروضة على الوصول لمكان ما. في النزاعات المسلحة، يمكن تعبئتها بدلًا من الباحث.

» **التأريخ:**
عادةً ما تتيح صور الأقمار الصناعية للباحثين السفر عبر الزمن للماضي لدراسة التغيرات على الأرض عن طريق البحث على المنصات العامة مثل جوجل إيرث.

» **المرئيات:**
يمكن لصور الأقمار الصناعية أن توفر مرئيات قوية ومؤثرة للاستخدام في حملات حقوق الإنسان وأعمال المناصرة وكسب التأييد.

» **موثوقية المصدر وإتاحة الميتاداتا:**
بالمقارنة بوسائل التواصل الاجتماعي، عادةً ما يكون المصدر الأصلي لصور الأقمار الصناعية واضحًا. كما أنها عادةً ما تأتي مع ميتاداتا مفصلة مثل الإحداثيات والتاريخ والوقت، مما يجعلها مصدرًا موثوقًا للبيانات.

» **التحليل المتقدم:**
ترصد حساسات الأقمار الصناعية معلومات أكثر من العين البشرية، مثل الأشعة تحت الحمراء أو فوق البنفسجية، والتي يمكن استخدامها لتمييز الكساء الخضري وقياس صحته. يمكن لهذه التقنيات أن تستخدم، على سبيل المثال، لقياس أثر التسرب النفطي وعرضه بصريًّا أو لتوثيق آثار التحركات العسكرية أثناء النزاع المسلح أو لقياس العنف البيئي بوصفه مؤشرًا على الإبادة الجماعية.

محدوديات صور الأقمار الصناعية:

» **التفسير:**
يمكن لتحليل الصور أن يكون عرضة لسوء التفسير، خاصة إذا ما اضطلع بهذا الأمر محللون أو باحثون لم يتدربوا على تحليل صور الأقمار الصناعية. على سبيل المثال، يمكن تفسير عدم استواء التربة إما بوصفه مقبرة جماعية وإما حديقة خضراوات. وبالتالي، فإن التأييد والتحقق باستخدام معلومات أخرى هو أمر جوهري.

» **الإتاحة:**
لا ترصد الأقمار الصناعية التجارية أو الحكومية كل موقع على الأرض على الدوام، ويمكن أن تكون هناك فجوات بيّنة في الصور المتاحة للمواقع، وبالتحديد في المناطق النائية أو الحساسة سياسيًّا.

» **السُّحُب:**
حتى لو كانت الصور متاحة في التاريخ المرغوب، فيمكن لتغطية السحب أن تعيق القدرة على استخدام الصور إلى حد بعيد.

» **مجالات الاستخدام:**
تفيد صور الأقمار الصناعية في مجموعة واسعة ومتنوعة من مجالات حقوق الإنسان، ولكن يمكن لها أن تكون ذات استخدام شديد المحدودية في مجالات أخرى تدعو للقلق. الاختفاءات القسرية، على سبيل المثال، يصعب أو يستحيل توثيقها من خلال صور الأقمار الصناعية.

دراسة الحالة

الكشف عن مذبحة وأعمال هدم في نيجيريا بواسطة صور الأقمار الصناعية

في أعقاب ظهور تقارير تتحدث عن عمليات قتل وهدم في زاريا بنيجيريا في ديسمبر/ كانون الأول ٢٠١٥، راجع محللون من العفو الدولية صور الأقمار الصناعية الموجودة على الإنترنت مجانًا من جوجل إيرث للعثور على دليل داعم على عمليات قتل واسعة النطاق ارتكبها الجيش النيجيري، مما كشف عن محاولة بدائية من قِبل السلطات لإخفاء الأدلة. لحسن الحظ، في هذه الحالة، احتوى جوجل إيرث على صور محدثة أمكن الوصول لها عن طريق شريط تمرير «عرض الصور التاريخية» في القائمة الموجودة أعلى اليسار. تتيح لك هذه الخاصية رؤية التغييرات التي طرأت على صفحة الأرض على مر الزمن. في حالة زاريا، ساعدت في التعرف على عدة مناطق مهدمة تضمنت مدفنًا ومسجدًا، بالإضافة إلى ظهور ما يبدو على الأغلب كمقبرة جماعية. استخدمت خاصية «حفظ الصور» لتحميل الصور التي استخدمت في التقرير. يمكن استخدام كل صور جوجل إيرث مجانًا لأغراض غير تجارية. يتيح شراء نسخة برو من جوجل إيرث تحميل صور عالية الوضوح تكون أفضل في الطباعة.

لدعم الأثر البصري لصور الأقمار الصناعية في تقارير الإنترنت، يمكن إنشاء شريط تمرير بسيط يتيح للقارئ استكشاف التغيرات الوقتية بنفسه. إحدى الأدوات المجانية والسهلة لإنشاء شريط تمرير مدمج هي Juxtapose (جوكستابوز).

المثال الأول: هدم مسجد

قبل الهدم :
https://c2.staticflickr.com/856_26656228073/7754/a3c2f374_c.jpg)

بعد الهدم:
https://c2.staticflickr.com/89774490_27261977225/7236/f7e_c.jpg

المثال الثاني: مقبرة جماعية

قبل:
https://c2.staticflickr.com/21713948455_25903760253/1507/_c.jpg

بعد:
https://c2.staticflickr.com/2717_25901693544/1704/cff591d_c.jpg

انظر شرائط التمرير التي تنتقل من صور «قبل» إلى صور «بعد» لجميع المواقع على مدونة جوجل إيرث.

المثال الأول: هدم مسجد

المثال الثاني: مقبرة جماعية

مصادر صور الأقمار الصناعية التي يصل وضوحها إلى متر بحد أدنى

» **جوجل إيرث:**
يمكن أن يكون أداة عظيمة الفائدة لجمع صور الأقمار الصناعية المجانية. ولكن أحيانًا ما يقل وضوح الصور في بعض المناطق نتيجة للضغط السياسي.

» **TerraServer – تيرا سيرفر:**
أحد موردي صور الأقمار الصناعية من ديجيتال جلوب. يمكن استخدامه مجانًا، دعمًا للأبحاث الأساسية، وعادةً ما يوفر صورًا أكثر تحديثًا من جوجل. ينبغي أن تدفع رسمًا بسيطًا في مقابل تحميل الصور الفعلية. كما أنك لا بد وأن تدفع في مقابل الحصول على ترخيص إذا ما رغبت في استخدام الصور بشكل علني.

» **موردو الصور التجارية:**
الموردون الأساسيون لصور الأقمار الصناعية شديدة الوضوح والمتاحة تجاريًّا هم DigitalGlobe (ديجيتال جلوب) وAirbus (آير باص) وUrthecast (يورثاكاست) وDeimos-2 (ديموس-٢). يتراوح وضوح هذه الأقمار الصناعية بين ٠,٣ و٠,٧٥ متر (تقريبًا أصغر حجم لشيء يمكن التعرف عليه في صورة). الحد الأدنى لحجم الطلب عند شراء الصور هو ٢٥ كيلومترًا مربعًا. تبدأ أسعار هذا الحجم من ١٧٥ دولارًا تقريبًا.

» **الأقمار الصناعية متناهية الصغر:**
إحدى المميزات الكبيرة للشركات من أمثال Planet Labs (بلانِت لابز) أو TerraBella (تيررا بِلّا) هي أنها في نهاية المطاف ستوفر كوكبة كاملة من الأقمار الصناعية، وذلك يعني أنها تعمل على إنشاء نظام للرصد المستمر من الفضاء، ولكن الشركات المذكورة عاليه يمكنها فقط أن توفر لقطات لمناطق معينة على الأرض. ترقب صدور مقاطع فيديو الأقمار الصناعية، والتي سيكون لها آثار كبيرة على أبحاث حقوق الإنسان. ولكن أحد عيوب هذه الأقمار الصناعية متناهية الصغر هو أن معظمها حاليًّا ينتج صورًا منخفضة الوضوح، أي أن هناك تفاصيل أقل تظهر في الصورة.

اعتبارات البيانات المسئولة

المخاطر المتعلقة بالسلامة على أرض الواقع

يتطلب كل من الأمن والسلامة الجسديين في سياق البيانات الرقمية رؤية ونهج مختلفين. بالنسبة لأساليب جمع التوثيق التقليدية، فإن الحقوقيين المحترفين عادةً ما يتبعون أفضل الممارسات البديهية لحماية أنفسهم والأفراد الذين يجرون معهم المقابلات: اللقاء في مواقع مؤمنة والإبقاء على سرية المعلومات التعريفية وتجنب تعريض النفس للخطر بصورة مباشرة.

ولكن لا يعتبر الأمن الجسدي فيما يتعلق بأساليب البيانات الجديدة بالنسبة للكثيرين من البديهيات حتى الآن، لأنه عادةً ما لا تكون هناك علاقة شخصية بين الباحث والأفراد المُشار إليهم في البيانات.

هناك صلة وثيقة بين الأمن الجسدي والرقمي. الهدف من الأمن الرقمي ليس حماية البيانات وحسب، ولكن أيضًا حماية الأفراد الذين أسهموا في تكوينها أو ظهروا فيها.

إذا ما عرّض أحد قراصنة الإنترنت الخادم للخطر، أو إذا ما صادر مسئول أحد الكمائن قرصًا صلبًا، تُعَرَّض أسماء ووجوه و/ أو معلومات عدد كبير من الضحايا أو الأفراد الضعفاء للخطر. واجبك يحتم عليك أن تتخذ خطوات لحماية نفسك والآخرين من الضرر الإضافي.

يندرج المرتبطون بالبيانات تحت ثلاث فئات، أحيانًا ما تتداخل: من يلتقطون البيانات، ومن يشاركونها على الإنترنت أو على قرص صلب خارجي، ومن توجد معلوماتهم بداخل البيانات.

غالبًا ما لا يدرك الناس أن مقطع الفيديو الذي ينشرونه على الإنترنت يحتوي على معلومات حساسة. إذا ما قررت، بوصفك من العاملين في مجال حقوق الإنسان، استخدام مقطع فيديو لحملة، فقد يتم استهداف مصدر الفيديو ومنشئه على أساس ارتباطهما بمجموعتك، حتى لو لم يسمعا بك أبدًا.

قد لا يكون من ظهروا في المحتوى قد وافقوا على أن يتم تصويرهم، وربما لم يكونوا على دراية بأنه يتم تصويرهم من الأساس. إذا ما كشفت عن وجوههم أو أسمائهم في سياق انتهاك لحقوق الإنسان، فربما تتسبب دون قصد في تعرضهم للتحرش أو للمزيد من الإيذاء.

في حالة نشرك للبيانات، أو في حالة حدوث اختراق خارجي، قد يزيد خطر تعرض المصدر والأفراد الظاهرين في المحتوى للإيذاء الجسدي، حتى لو كانت معلوماتهم موجودة بالفعل من قبل على الإنترنت. والأسوأ من ذلك هو أنه قد يصعب إبلاغ أي من الأفراد المعرضين للخطر بتزايد عنصر الخطورة، لأن الباحث غالبًا ما لا يمتلك معلومات اتصال أو أي سبل للوصول إليهم. لذا فإن تجنب إذاعة البيانات منذ البداية هو أمر حيوي.

دراسة الحالة

الهندسة الاجتماعية: من الذي تتحدث إليه حقا عبر الإنترنت؟

يوفر النشاط الحقوقي في إيران مثالاً جليًّا على الصلة بين الأمن الرقمي والجسدي. مؤخرًا، استغلت السلطات الإيرانية الهندسة الاجتماعية لاستهداف المناصرين الحقوقيين من خلال الاتصالات عبر البريد الإلكتروني والفيسبوك ولينكد إن. الهندسة الاجتماعية هي فكرة استخدام الحقائق الشخصية والتلاعب النفسي لإقناع فرد ما بأمان خرق بروتوكولات الأمن والإفصاح عن المعلومات الشخصية. يمكن لأحد عملاء الحكومة أن ينشئ حسابًا على إحدى وسائل التواصل الاجتماعي باستخدام اسم ناشط معروف ويبدأ محادثات تخدع ناشطين آخرين وتؤدي بهم إلى الكشف عن معلومات حساسة.

استخدمت الجمهورية الإسلامية هذا التكتيك بنجاح كبير، مما أدى إلى اعتقال مناصرين حقوقيين بارزين واستجوابهم. وحتى مسئولو الحكومة الأمريكية قد وقعوا فريسة للهندسة الاجتماعية، حيث أفصحوا عن غير عمد عن معلومات للحكومة الإيرانية. عادةً ما تكون الهندسة الاجتماعية أكثر فعالية من القرصنة التقليدية لأنها لا تعتمد على أي مهارات تقنية وتعتمد على نقاط ضعف الأفراد وليس النظم الرقمية.

لتجنب التعرض لهجمات تقنيات الهندسة الاجتماعية، كن متيقظًا في جميع اتصالاتك. اسأل أسئلة موضحة أو شخصية لضمان أن من تتحدث إليه هو من يدعي بالفعل، واقطع الاتصال إذا ما راودتك أي شكوك بشأن هوية صاحب الحساب. أيضًا تجنب مشاركة المعلومات الحساسة على وسائل التواصل الاجتماعي أو البريد الإلكتروني بدون وجود إجراءات أمنية أخرى قائمة.

البيانات المسئولة

البيانات المسئولة هي:

الالتزام بكفالة حقوق الناس في الموافقة والخصوصية والأمن والملكية فيما يتعلق بعمليات المعلومات من جمع وتحليل وتخزين وتقديم وإعادة استخدام للبيانات، مع احترام قيم الشفافية والانفتاح في الوقت ذاته.

-(منتدى البيانات المسئولة، التعريف الرسمي، سبتمبر/ أيلول ٢٠١٤)

لتظل على اطلاع بالمستجدات فيما يتعلق بالبيانات المسئولة، انظر https://responsibledata.io واشترك في القائمة البريدية على https://engn.it/rdmailinglist

» **تقليل البيانات للحد الأدنى:**
في سبيل الخصوصية وتقليل عنصر المخاطرة، حاول دائمًا أن تجمع الحد الأدنى من البيانات اللازمة لهدفك المحدد.

» **البيانات الشخصية:**
كلما أمكن، إذا ما كانت لديك أسماء أو تواريخ ميلاد أو أي معلومات تعريفية شخصية، حاول تجهيلها أو مسح ما لا تحتاجه.

» **البيانات الحساسة:**
تنبه إلى مكان تخزين البيانات الحساسة الخاصة بالعِرق أو التوجه الجنسي، سواء على خوادمك الخاصة أو في بلد أجنبي، (مثلًا عن طريق استخدام خدمة جوجل) لإمكانية تعريض الأفراد للخطر عن طريقها.

» **التحيز الضمني:**
قد تحتوي البيانات المجموعة من مصادر أخرى على تحيزات خفية. فكر مليًّا في القرارات البشرية التي اتخذت أثناء التحليل.

إن مراعاتك للغير وتمتعك بروح المبادرة فيما يتعلق بعملك مع البيانات الرقمية لهما صفتان لا غنى عنهما لكفالة سلامة من تعمل معهم. يمكن الحديث عن المسائل الأخلاقية التي قد تنشأ في هذا السياق تحت مظلة تحديات البيانات المسئولة. لا توجد سياسة واحدة ستنجح في جميع المواقف، ولكننا نشجعك على التفكير في الموضوعات التالية كما يتوافق وسياقك:

» **الموافقة المستنيرة:**
بالتحديد في سياق انتهاكات حقوق الإنسان، تعني الموافقة المستنيرة أكثر بكثير مما تظن. تأكد من أن من يعطونك الموافقة قد قاموا بهذا الأمر بشكل طوعي، وأنهم يفهمون تمامًا ما يوافقون عليه، بالإضافة إلى كونهم في موقف يسمح لهم باتخاذ مثل هذه القرارات.

المعلومات المجموعة من وسائل التواصل الاجتماعي

يبدو وكأن الكثير من المنظمات تعتقد أن المعلومات الموجودة «في المجال العام» متاحة للاستخدام لأي غرض. ولكن، حتى لو أن أحدهم قد وافق على وضع معلوماته في المجال العام بشكل معين، فإن ذلك لا يعني بالضرورة أنه من الأخلاقي الاستيلاء على المعلومات لأي استخدام.

عندما ينشر شخص ما شيئًا يتعلق بانتهاك حقوق الإنسان على تويتر، لا يعني ذلك أنه يوافق تلقائيًّا على أن يصبح النقطة المركزية لحملة حقوقية عالمية النطاق. لا بد وأن تتواصل مع الأشخاص مباشرة وأن تساعدهم على فهم العواقب المحتملة (الإيجابية والسلبية) لجذب المزيد من الاهتمام، حتى يتمكنوا من اتخاذ قرار مستنير.

حماية هوية الأفراد على وسائل التواصل الاجتماعي

قد تحتوي منشورات وسائل التواصل الاجتماعي التي توثق الانتهاكات على مقاطع فيديو و/ أو صور لأفراد لم تكن لديهم أدنى فكرة أنه يتم تصويرهم. سواء كنت أنت من تنشر هذه البيانات، أو منظمة ترغب في إعادة نشرها، لا بد من أن تحمي الأفراد بأكبر قدر ممكن.

توجد العديد من الأدوات المفيدة للتشويش على الوجوه في الفيديو والصور. على سبيل المثال، ObscuraCam (أوبسكيورا كام) هو تطبيق لهواتف الآندرويد يقوم ببكسلة أو حجب الوجوه. ويمكن استخدامه إما عند التسجيل وإما عند رفعك للمحتوى عليه من مكتبتك. كما أضاف يوتيوب مؤخرًا خاصية التعتيم التي تتيح لك طمس الوجوه عند رفعك لمقطع فيديو.

هل أدواتك الرقمية في أمان؟

حينما يتعلق الأمر بإنشاء نُسخ احتياطية والتخزين الآمن للملفات والتدمير الآمن للبيانات، نوصي باستشارة (الأمن في صندوق) من تكتيكال تيكنولوجي كوليكتيف وفرونت لاين ديفندرز.

لا يقتصر الأمن الرقمي على استخدام الأدوات والبرمجيات الآمنة، ولكنه جزء لا يتجزأ من العادات والممارسات التنظيمية العامة.

وعندما نتحدث عن الأمن الرقمي، فإن ذلك يشتمل على اتخاذ خطوات لحماية البيانات سواء أثناء الانتقال (البريد الإلكتروني ومحادثات الدردشة وخدمة الرسائل القصيرة) وأثناء الكمون (ملف محفوظ على قرصنا الصلب).

ونحن نتخذ هذه الخطوات لأنه أثناء جمع البيانات الحساسة والاحتفاظ بها ومشاركتها، وبخاصة فيما يتعلق بالبيانات المرتبطة بحقوق الإنسان، توجد نتائج تتعلق بالأخلاقيات والأمان.

تقع على عاتقنا مسئولية حماية خصوصية أولئك الذين تُمثل أسماؤهم وهوياتهم في بياناتنا، والذين يضعون ثقتهم فينا بتوفير معلوماتهم.

تقدم الأدوات والخدمات الجديدة ادعاءات متنوعة بشأن أمن منتجاتها. كيف نتأكد من صحة ذلك؟ هذه هي بعض الأسئلة التي يجب أن نطرحها عند النظر في استخدام برنامج جديد. على الأغلب لن تتمكن من الإجابة عنها جميعًا، ولكن حاول بقدر الإمكان.

قبل استخدام برنامج جديد، اسأل نفسك:

١. ما الذي تعنيه حقًّا كلمة «آمن»؟

قد يعني القول إن أحد البرامج «آمن» العديد من الأشياء. اقرأ الشروط والأحكام الدقيقة لوصف أي برنامج. الكثير من الأدوات التي تدعي كونها «آمنة»، بما يشتمل على دروب بوكس وجوجل وسكايب، تشفر بياناتك أثناء سفرها فيما بين حواسبك وخوادمها – ولكن البيانات لا تكون محمية من الوصول إليها بواسطة الشركات نفسها. اسأل دائمًا عن كيفية حماية الخدمة لبياناتك. تستخدم بعض الأدوات والخدمات التشفير بطرق تحمي البيانات حتى من مقدمي الخدمة أنفسهم. من الأهمية بمكان فهم هذا الفصل، والنظر في ما إذا كان من المهم لمشروعك أن يتم إخفاء البيانات عن مقدمي الخدمة.

٢. هل تم تدقيق البرنامج بصورة مستقلة؟

لا تثق في مطوري البرمجيات حينما يَعدون بتقديم الأمن، خاصة عندما يكون البرنامج جديدًا جدًّا. حتى مع توفر أفضل النوايا، فإن تنفيذ التشفير بشكل صحيح أمر صعب. استخدم فقط البرمجيات التي تم تدقيقها بشكل مستقل على يد من تثق به. من الأفضل أن تكون شفرة البرنامج «مفتوحة المصدر» ومتاحة للفحص العام. وحتى وقتئذ، لا يمكنك التأكد تمامًا من عدم إغفال عمليات التدقيق النظيفة لأي ثغرات. لا بد من استخدام الشك الصحي باستمرار.

٣. من يمتلك البيانات – ولِكم من الوقت؟

عند استخدامك لخدمة إلكترونية لإيصال المعلومات أو إنشائها أو أرشفتها، لا بد أن تسأل عمّن «يمتلك» البيانات، خاصة لو كانت مخزنة على خوادم مقدم خدمات مثل فيسبوك أو تويتر أو دروب بوكس. عادةً ما تكون الإجابات مدفونة في شروط الخدمة الخاصة بالشركة. أيًّا كانت الخدمة التي تستخدمها لأرشفة البيانات الحساسة أو مشاركتها، لا بد وأن تقوم بالبحث في سياساتها بشأن مشاركة البيانات مع الشركات أو الحكومات الأخرى، وفيما ينبغي عليك أن تتوقع حدوثه للبيانات في حال مسحك لحسابك أو إذا ما بيعت الشركة أو أغلقت.

٤. هل يقدم البرنامج حماية من التهديدات المحددة التي تواجهك؟

فهم التهديدات التي تواجهك بشكل خاص مهم لتقييم ما إذا كان التطبيق أو الخدمة المبتغاة سيقومان بحمايتك على النحو المناسب. بدلًا من استخدام أداة لأنك سمعت أن ذلك هو ما يجب أن تفعله، حاول بناء «نموذج للمخاطر» لتحديد من قد يحاول الوصول إلى بياناتك، وكيف سيفعل ذلك (انظر دليل الدفاع عن النفس ضد الرقابة: مقدمة إلى نمذجة التهديدات). سوف تساعدك الإجابة عن هذه الأسئلة في تحديد أكثر الأدوات أهمية. لتعلم المزيد بشأن القيام بتحليل السياق، انظر قسم الاستكشاف Explore (في دليل الأمن الشمولي).

٥. هل سيتسبب استخدامك للبرنامج أو الخدمة في الكشف عنك؟

في بعض الأماكن، يُعد استخدام التشفير عملًا غير قانوني، بينما قد لا يكون الأمر كذلك في أماكن أخرى، ولكنه قد يسترعي الشكوك من جانب وكالات إنفاذ القانون أو الاستخبارات. قد يؤدي ذلك بهم إلى أن يبدءوا في رصد نشاط شخص ما ببساطة لأنه بدأ في استخدام برمجيات الأمن أو التشفير. من الأهمية بمكان فهم المخاطرة التي قد تتعرض لها؛ في بعض السياقات، قد يكون الخيار الأكثر أمنًا هو عدم استخدام التشفير، على الرغم من أن البيانات سوف تخزن وتُرسل بلا حماية (وذلك أيضًا يمثل مخاطرة!)، قد يساعدك ذلك على تجنب لفت الأنظار واجتذاب الانتباه. معرفة سياقك هي أمر لا غنى عنه عند إجرائك لمثل هذا النوع من التقييم.

٦. هل سيمثل استخدامك لهذه الخدمة أو البرمجيات خيارًا عمليًا؟

قد تتناسب بعض البرمجيات أو الخدمات بشكل جيد مع العمليات القائمة التي تستخدمها لجمع البيانات وتحليلها ومشاركتها. قد يتطلب البعض الآخر نقلة جوهرية لعمليات جديدة. حتى فيما يختص بالبرمجيات التي تَعد بالأمن، تمثل صفة العملية عنصرًا هامًا. إذا كان استخدام البرنامج أصعب من اللازم أو من المرجح ألا يصبح ممارسة مستدامة، فإن محاولة استخدامه قد تسفر عن ضياع للموارد الثمينة من وقت ومال وطاقة.

٧. هل تستخدم هذا التطبيق للأسباب الصحيحة؟

توجد العديد من الأسباب التي قد تثير اهتمامنا بخدمة أو أداة جديدة: جمال التصميم، جاذبية الاسم، الوعد بخدمة مستحدثة، الرواج المتزايد، إلخ...، انظر نظرة نقدية متعمقة نحو الأسباب التي تعتقد أنها تدعوك إلى استخدام الأداة، وتأكد من كونها الأسباب الصحيحة، واضعًا في الحسبان احتياجاتك والتزاماتك الأخلاقية والأمنية.

من النادر جدًا أن يلبي أي برنامج أو خدمة جميع هذه الاحتياجات. ليس الهدف هو أن نجد بيضة الديك التي تلبي جميع المتطلبات، ولكن ما نبتغيه هو اتخاذ قرارات مستنيرة ومقصودة بشأن البرمجيات التي نستخدمها. بعد قراءة هذه النصيحة، هل اختلف إحساسك بشأن أي أداة أو خدمة بدأت في استخدامها مؤخرًا؟ هل مازالت هي الخيار الصحيح بالنسبة لك؟

في العمق

الصراحة بشأن نقاط الضعف

ينشر بعض المطورين «نماذج المخاطر» ونقاط الضعف المعروفة على مواقعهم الإلكترونية من أجل الشفافية. للحصول على أمثلة جيدة، انظر توثيق كل من Scramble.io (سكرامبل) (برنامج آمن للبريد الإلكتروني) وCryptocat (كريبتوكات) (برنامج دردشة آمن). كما تنشر المزيد من الشركات الآن تقارير الشفافية التي توضح أشياء مثل الطلبات الرسمية لمعلومات المستخدمين وإشعارات الإزالة القانونية، انظر تقرير شفافية تويتر. هذه التقارير طوعية ويصعب التحقق منها، ولكن بالرغم من ذلك، فإنها تقدم سياقًا حول أمان الخدمات.

المثال

هل يستخدم جون الواتساب للعمل الحقوقي؟

جون ناشط حقوقي في كامبالا بأوغندا، ويجمع تقارير عن العنف ضد المثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسانية وحاملي صفات الجنسين. المثلية الجنسية غير قانونية في أوغندا، ومجموعة جون تخضع لرقابة الشرطة بشكل دوري. اشترى جون للتو أول هاتف ذكي، وينظر في استخدام تطبيق واتساب للدردشة، حيث يستخدمه العديد من أصدقائه، كما أنه قد سمع أنه تطبيق آمن.

وهذا هو ما قرره جون...

طبق الواتساب تشفير سيجنال الذي يتمتع بالكثير من الثقة في أوساط المستخدمين في 2016، وهو تشفير مفتوح المصدر وقابل للتحقق. ولكن تطبيق واتساب نفسه ليس مفتوح المصدر ولا توجد تدقيقات عامة لشفرته، لذا فلا يمكن لجون أن يتأكد كليةً من أمنهما. كما أن رسائل الواتساب تُشفر أثناء الانتقال، وليس على الجهاز، لذا فقد يمثل الهاتف حال سرقته نقطة ضعف. لا يستبعد جون استخدام واتساب بشكل كامل، ولكن يسأل زميلًا له، ويقرر أن يبحث في تطبيقات الرسائل الأخرى، ومنها Openevsys (أوبن إيف سيس) و Martus (مارتوس) المطوران لأغراض حقوق الإنسان.

الصدمة الثانوية واضطراب كرب ما بعد الصدمة

يلتزم العاملون في مجال حقوق الإنسان بمساعدة الآخرين، وبناءً عليه، فإنه عادة ما ينظر إلى حرصهم على الأمن والسلامة بوصفه هدفًا أنانيًّا أو من الرفاهيات، وخاصة عند العمل في مناطق النزاع. من الأهمية بمكان أن يعمل كل من المنظمات والأفراد على التصدي لهذا المعتقد الخاطئ. إن الاعتراف بأهمية الأمن والسلامة يوطد من أواصر الصمود وخفة الحركة، كما أنه يحسن من إدارة الموارد وتعبئتها، ويتيح التحضير للمخاطر، الذي هو جزء أصيل من العمل في مجال حقوق الإنسان.

يتعلق الأمن بالسلامة الجسدية والصحة والماليات والتمييز والخصوصية، إلخ...، تختلف مخاطر الأمن من شخص إلى آخر ومن مجموعة إلى أخرى. بالنسبة للبعض، قد يمثل الدين أو التوجه الجنسي أكبر المخاطر على سلامتهم. ويُعد تفهم هذه المخاوف من وجهة نظر كل المنخرطين في عملك الخطوة الأولى نحو تهيئة بيئة منتجة وآمنة.

سيساعدك إجراء التحليل التالي والمحافظة عليه على التأسيس للاستراتيجيات والخطط والاتفاقيات المشتركة لدعم الأمن والسلامة:

- استكشف التطورات السياسية والاقتصادية والاجتماعية والتكنولوجية والقانونية والبيئية ذات الصلة المحورية بعملك.
- تعرف على المخاطر الفعلية على السلامة وحللها واتخذ الخطوات اللازمة لمنعها أو التصدي لها.
- حدد حلفاءك وخصومك: مصالحهم وقدرتهم على تمكينك أو العمل ضدك.
- ارسم خريطة للمعلومات والبيانات الخاصة وصنفها واتخذ إجراءات لحمايتها من الضياع أو التلف.

إبطال مفعول الصدمة الثانوية من بياناتك

للكم غير المسبوق من المحتوى السمعي البصري المتاح لباحثي حقوق الإنسان اليوم الكثير من المزايا والكثير من المخاطر. أظهر البحث الذي أجراه Eyewitness Media Hub (آي ويتنس ميديا هَب) أن ٨٢٪ من باحثي حقوق الإنسان يشاهدون صورًا مؤلمة بينما يجلسون إلى مكاتبهم عدة مرات شهريًّا.

اعتبارات البيانات المسئولة

يمكن للتعرض للكثير من الصدمات الأولية أن يؤدي إلى الصدمة الثانوية، والتي يمكن بدورها أن تؤدي إلى اضطراب كرب ما بعد الصدمة. لا بد للمنظمات والمديرين والباحثين التعرف على هذه المخاطر والحد منها. وضع Eyewitness Media Hub قائمة بعدة مؤثرات يمكن أن تكون مؤلمة بالنسبة للأفراد، والعديد منها شائعة في مصادر البيانات الرقمية، بما يشمل:

- **المفاجأة:** لا يتوقع الفرد مشاهدة العنف في مقطع الفيديو.
- **التعرض المتكرر:** ينبغي على الفرد مشاهدة مقطع فيديو عنيف بشكل متكرر.
- **الربط الشخصي:** يذكر المحتوى الباحث بموقف شخصي أو رابط شخصي.
- **صوت إنسان يعاني:** يجعل سماع صوت العنف الفيديو أكثر إيلامًا.
- **الإحساس بالذنب:** يورد باحثو حقوق الإنسان إحساسًا دائمًا بالذنب نتيجة لإحساسهم بالصدمة بسبب العنف الممارس على شخص آخر.

التعرف على الصدمة الثانوية

- صعوبة في إدارة مشاعرك.
- صعوبة في تقبل ذاتك أو الرضا عنها.
- صعوبة في اتخاذ قرارات جيدة.
- مشاكل تتعلق بإدارة الحدود الشخصية. مثال: تحمل مسئولية أكبر من اللازم، صعوبة في مغادرة العمل في نهاية اليوم، محاولة التدخل في حياة الآخرين والتحكم بها.
- مشاكل في العلاقات.
- مشاكل جسدية مثل الأوجاع والآلام والأمراض والحوادث.
- صعوبة الشعور بالارتباط بما يحدث حولك وداخلك.
- فقدان المعنى والأمل.
- زيادة التعاطي، وخاصة الكحول.
- النهم في تناول الطعام.
- عزل النفس عن الأصدقاء والزملاء.

قد يستشعر الأفراد الذين يمرون بالصدمة الثانوية بعض هذه الأعراض أو كلها، وربما لا يستشعرون أيًّا منها. يجب التدقيق في أي تحولات سلوكية مفاجئة.

خطوات فورية لتجنب الصدمة الثانوية:

١. باعد ما بين المرات التي يتعرض فيها الموظفون إلى المحتوى الصادم.

٢. تخلص من التعرض المتكرر للمؤثرات بدون داعٍ.

٣. راجع إجراءات التصنيف والتوسيم لتقليل المشاهدات غير الضرورية.

٤. جرب طرقًا مختلفة للمشاهدة. يجد البعض أن التركيز على تفاصيل معينة مثل الملابس، وتجنب أخرى (مثل الوجوه) يمكن أن يساعدهم في خلق مسافة عاطفية.

٥. عدّل من بيئة المشاهدة: قلل حجم الصورة أو الفيديو أو عدل درجة إضاءة/ وضوح الشاشة.

٦. أطفئ الصوت عند الإمكان.

٧. خذ استراحات متكررة من الشاشة. انظر إلى شيء لطيف، أو تمشى أو تمطى.

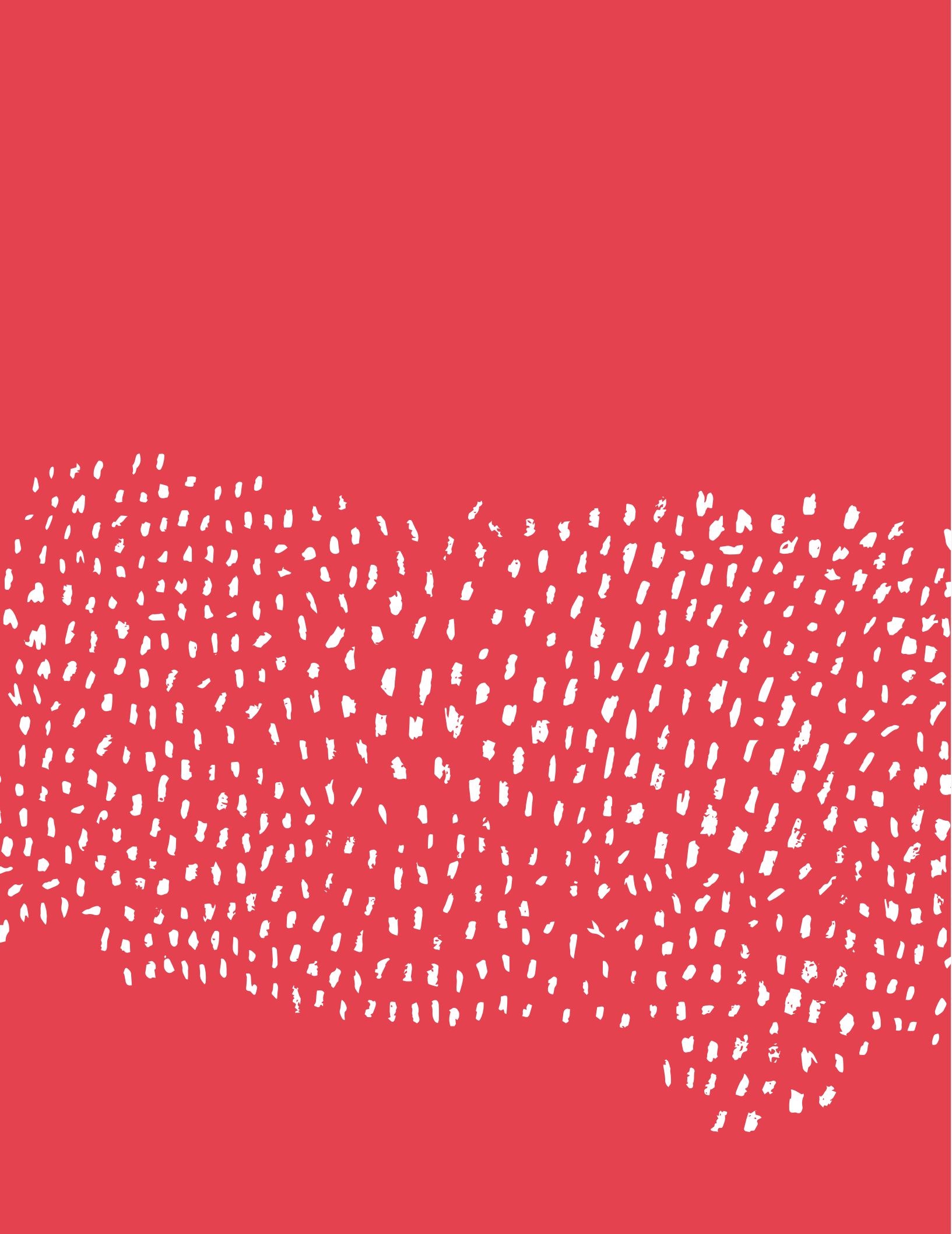
٨. عند إرسال محتوى عنيف عبر البريد الإلكتروني، اكتب تحذيرًا في خانة الموضوع.

٩. ضع علامة واضحة على جميع الملفات عند الأرشفة حتى لا يتعرض الناس عَرَضًا للمحتوى العنيف.

١٠. صمم خطتك الخاصة للعناية الذاتية. يظهر البحث أن الأفراد الذين يتمتعون بالكثير من الصلابة غالبًا ما يمارسون الأنشطة الرياضية بشكل دوري، ويحافظون على اهتماماتهم وما يثير حماستهم خارجيًّا، ويستثمرون الوقت في روابطهم الاجتماعية عند مواجهتهم لتحدي الإجهاد المتصل بالصدمة.

١١. أسس شبكات لدعم الأقران بداخل المنظمات للحديث عن المحتوى الشنيع الذي اضطررت للتعامل معه.

إن اضطراب كرب ما بعد الصدمة الناتج عن الصدمة الثانوية قابل للعلاج. إذا كنت تعتقد أنك أو أحد زملائك تعانيان من اضطراب كرب ما بعد الصدمة، اسع للحصول على المساعدة من خبير على الفور.



إلى أين تذهب بدءًا من هنا؟

كيف تؤطر بحثك؟

قبل الولوج إلى التحليل، فكر مليًّا فيما تمثله بياناتك وفي الاستخلاصات السليمة التي يمكنك الخروج بها منها. يساعد هذا القسم على تحديد مدى تمثيل مجموعات البيانات وتعيين أوجه الشك فيها لتجنب الاستخلاصات غير اللائقة أو غير السليمة.

تحديد نوع العينة التي تمثلها بياناتك

هناك ثلاثة أنواع من العينات. يعتمد نوع العينة الموجودة لديك على عدد وحدات التحليل الموجودة لديك وكيفية اختيارها.

- **العينة الكاملة:** مجتمع إحصائي كامل. «تعداد سكاني» أو «إحصاء كامل» هما تعبيران آخران يدلان على العينة الكاملة.
- **العينة الاحتمالية:** اختيرت وحدات من المجتمع الإحصائي من خلال آلية احتمالية. تكفل هذه الآلية معرفة احتمالية الاختيار لكل وحدة في المجتمع الإحصائي.
- **العينة الملائمة:** اختيرت الوحدات بآلية غير احتمالية. احتمالية الاختيار في العينة بالنسبة لكل وحدة في المجتمع الإحصائي غير معروفة، حيث ترتفع للغاية بالنسبة لبعض الوحدات وتنخفض جدًّا أو تصل للصفر لوحدات أخرى. في أبحاث حقوق الإنسان، غالبًا ما تكون عينات البيانات المتاحة هي العينات الملائمة.

تحديد الاستخلاصات التي يمكنك التوصل إليها

تسمى عملية التعلم والوصول لاستخلاصات من البيانات بـ«الاستنباط». يوجد نوعان من الاستنباط:

الاستنباط الإحصائي يتوصل لاستخلاصات بشأن المجتمع الإحصائي، بناءً على العينة. وهذه الاستخلاصات تُعد صالحة فقط إذا ما كانت لديك عينة كاملة أو احتمالية.

الوصف يتوصل لاستخلاصات بشأن العينة الموجودة لديك.

الاستنباط من عينة كاملة

العينات الكاملة تتميز بكونها مماثلة للمجتمع الإحصائي، لذا فإن أيًّا ما تعرفه عن العينة ينطبق أيضًا على المجتمع الإحصائي.

الاستنباط من العينة الاحتمالية

العينات الاحتمالية ممثلة للمجتمع الإحصائي إذا ما أخذت احتماليات العينات الضمنية في الحسبان. لأن كل وحدة في المجتمع الإحصائي لديها احتمالية معروفة للاختيار كجزء من العينة، ففي المتوسط يمكننا تقريب نفس القيم والتوزيعات في عينتنا الموجودة في المجتمع الإحصائي (ناقص خطأ أخذ العينات الاحتمالية). لا نضع في الاعتبار جميع الوحدات في المجتمع الإحصائي، ولكن فقط عينة تمثيلية، وبالتالي، فإننا نسمي هذه الاستخلاصات «التقديرات».

في العمق

المجتمع الإحصائي

في الإحصائيات، يشير المجتمع الإحصائي إلى جميع وحدات التحليل التي تريد دراستها.

المثال الأول:
ترغب في معرفة كم من اللاجئين الذين دخلوا البلد ص بالقوارب يتم حرمانهم من الرعاية الصحية. المجتمع الإحصائي يتكون كله من اللاجئين الذين وصلوا إلى البلد ص بالقوارب وتم حرمانهم من الحصول على الرعاية الصحية.

المثال الثاني:
تقوم بفحص لمعرفة ما إذا كانت زراعة الزهور التجارية قد تسببت في تلوث المياه في منطقة بعينها. هنا، ص هي جميع حقول الزهور في تلك المنطقة.

العينات الملائمة

العينات الملائمة غير ممثلة للمجتمع الإحصائي: فهي متحيزة بطرق غير معروفة. جميع العينات الملائمة تحتوي على تحيز الاختيار. في الإطار الإحصائي، يعني ذلك أننا لا نعرف بشكل تام إلى أي مدى تمثل عينتنا المجتمع الإحصائي حقًّا. لا نعرف أي جزء من المجتمع الإحصائي لا يتسنى لنا رؤيته، وما هي النسبة التي يمثلها هذا الجزء بالنسبة للمجتمع الإحصائي، أو كيفية اختلاف عينتنا عنه.

الاستنباط من العينة الملائمة

العينات الملائمة ليست ممثلة للمجتمع الإحصائي؛ فهي متحيزة بطرق غير معروفة، لأننا لا نعلم أيًّا من وحدات المجتمع الإحصائي قد أهملت وأيها كان من المرجح أو المستبعد اختيارها. فيما يخص المجتمع الإحصائي ذا الصلة، لا يمكننا التعلم من هذه العينة، ويجب علينا ألا نبالغ في الاستخلاصات التي يمكننا التوصل إليها من خلالها.

الاستخلاصات التي يمكنك التوصل إليها عن طريق العينات الملائمة

- عدد الأشخاص الذين تمكنت من توثيقهم – من انتهك حقهم في الحصول على الرعاية الصحية.
- لخص وصِف الأفراد ذوي الصلة والمشاكل الصحية التي عانوا منها.
- ارسم مخططات بيانية لتصور الانتهاكات التي وثقتها. تأكد من تعريف هذه الرسوم بشكل واضح بوصفها ملخصات «للانتهاكات المُبلغ عنها» أو «الانتهاكات الموثقة». (انظر هذا التقرير من مجموعة تحليل بيانات حقوق الإنسان لتجد مثالًا عن كيفية وصف بيانات العينة الملائمة وكيفية إضافة الحواشي للمخططات البيانية الخاصة بالبيانات.)
- صِف ممارسات الدولة التي تعرفت عليها، والتي تؤدي إلى الحرمان من الحصول على الرعاية الصحية.
- اذكر أين ومتى تعرفت على هذه الممارسات. إذا ما كنت قد وثقت هذه الممارسات في عدة مرافق للرعاية الصحية في البلد ص و/ أو حدث ذلك بصورة متكررة على مر الوقت، فيمكنك أن تشير إلى هذا الانتشار المكاني و/ أو الزماني.

إلى أين تذهب بدءًا من هنا؟

» قم بالإشارة إلى أن غياب التقارير الإضافية عن ممارسات الدولة تلك لا يعني أن هذه الممارسات لم تحدث. ربما لم تتمكن ببساطة من التعرف على المزيد منها. لتأييد هذه العبارة، يمكنك أن تكتب قائمة بالمرافق التي لم تتمكن من زيارتها في محاولة لجمع المزيد من الأدلة. ربما لا يعني نقص الأدلة غيابًا للانتهاكات، بل يمكن أن يكون ببساطة نتيجة لعدم القدرة على البحث في هذا المجال.

» استخلص أن ممارسات الدولة هي أمر لا بد أن يؤخذ بجدية.

الاستخلاصات التي لا يمكنك التوصل إليها

» عدد اللاجئين المحرومين من الرعاية الصحية. لأن هذه العينة من النوعية الملائمة، فإنك لا تعلم عدد اللاجئين الذين لم تتمكن من توثيقهم.

» استنتج أيًّا من ممارسات الدولة هي الأكثر و/ أو الأقل شيوعًا.

» استنتج التوجهات المكانية عن طريق تحديد إذا ما كانت ممارسات الدولة أكثر شيوعًا في منطقة ما مقارنة بأخرى.

» استنتج التوجهات الزمنية عن طريق تحديد إذا ما كانت ممارسات الدولة قد حدثت بشكل أكثر تكرارًا أثناء فترة زمنية مقارنة بأخرى، و/ أو إذا ما كانت ممارسات الدولة قد زادت أو قلت أو ركدت على مر الزمن.

إذا ما عاملت معلومات عينتك الملائمة على هذا الأساس – أنها تمثل دليلًا على انتهاكات لحقوق الإنسان لم تتمكن من توثيقها – فسيكون لديك أساس متين لتأييد حججك الحقوقية في العلن.

توثيق عملية بحثك

» يجعل التخطيط الواضح لمنهجية وصولك لاستخلاص نتائجك أكثر إتاحة وشفافية، وفي الوقت ذاته يضفي صبغة الشرعية على حججك.

» يوفر التوثيق والأرشفة الداخليان الوقت والمال، وفي الوقت ذاته يقللان من خطر فقدان المعلومات.

» ينمي توثيق الممارسات الناجحة من معرفتك بداخل مجتمعك وخارجه. وتزيد أهمية ذلك الأمر مع مصادر البيانات الرقمية، حيث لم تزل القاعدة المعرفية في طور النمو.

» دون كل القرارات التي اتخذتها وارسم خارطة لمصادر البيانات التي استخدمتها. صِف كيف تحصلت عل كل مصدر من مصادر البيانات وكيف استخدمته.

» سيمكن الملخص المفصل خطوة بخطوة لمنهجية بحثك الآخرين من أن يحذوا حذوك، وأن يكرروا نتائجك، وأن يتوصلوا إلى استخلاصات مقارنة.

عينة من الأسئلة التي ينبغي أن تحاول منهجيتك الإجابة عنها

» **ما هو التركيز الجغرافي لدراستك؟**

» **ما هو التركيز الزمني لدراستك؟**

» **كيف قمت بقياس ص؟**

أ. مصدر بيانات #١

i. أين ومتى تم التحميل؟
ii. من هو المنشئ/ المورد الأصلي؟ هل هذا المصدر جدير بالثقة؟ كيف تحققت من هذه البيانات؟
iii. متاح للعامة؟
iv. هل قمت بترتيب البيانات نظاميًّا بشكل أو بآخر؟ على سبيل المثال بالساعة أو باليوم؟
v. هل ثمة قيود أو مخاوف أو تحديات تتعلق بهذه البيانات؟
vi. كيف تعاملت مع المعلومات الناقصة؟
vii. كلمات البحث المستخدمة، الهاشتاجات التي تمت متابعتها؟ بأي لغات؟

» **ما هي الطرق التي استخدمتها للتحصل على النتائج من البيانات المجموعة؟**

ب. معالجة البيانات وإدارتها

i. عملية الترجمة، إن وجدت.
ii. البرمجيات المستخدمة.
iii. عملية دمج/ ربط مصادر البيانات المختلفة.

ج. تحليل البيانات

i. لغات البرمجيات/ البرمجة المستخدمة.
ii. الطرق الإحصائية المستخدمة.
iii. الإجراء المتبع عند التعامل مع المعلومات المنقوصة.
iv. الأنواع المحتملة لاختبارات الدقة وتحليل الحساسية.

قبل استدعاء الخبراء.. جهز أسئلتك

يتمتع الباحثون اليوم بسهولة غير مسبوقة في الحصول على البيانات. ولكن العديد منهم لم يزل يفتقد إلى القدرات أو الثقة التي تؤهله لاستخدام مجموعات البيانات الكبيرة في إطار العمل. في مجال حقوق الإنسان ذي الموارد المالية الضئيلة والعمل المضني، يضع ذلك خبراء البيانات تحت ضغط شديد، حيث يجاهدون لتلبية طلبات زملائهم العديدة. كلما تعلمت المزيد عن عملك وتمكنت منه، وفرت المزيد من الضغط والوقت على نفسك وعلى زملائك.

ولكن بالرغم من ذلك، ففي بعض الأحيان يجدر بك استدعاء الخبراء. قبل أن تفعل ذلك، جهز نفسك للمحادثة التي ستُجرى عن طريق التدبر في الأسئلة التالية:

» **ما هو هدفك النهائي؟** يساعد توضيحك لأهدافك الخبير في فهم طلبك.

» **ما هو تعريفك للدعم الجيد؟** هل تبحث عن المساعدة لكي تفهم التحيز في مجموعة بيانات معينة؟ الدعم لتحليل مسار بيانات جديد بالنسبة لك. تأكيد على كونك على المسار الصحيح.

» **هل تحتاج إلى مساعدة معينة أم جارية؟** تحلَ بالواقعية واطلب فقط مقدار المساعدة الذي تستطيع تحمله.

» **لماذا هذا الخبير؟** هل اشتغل بحالات مماثلة من قبل؟ هل أوصى به أحدهم؟ هل فكرت في بدلاء؟

إلى أين تذهب بدءًا من هنا؟

قم بواجبك

ابحث عن مشروعات قامت بأشياء مماثلة لما تريد أن تفعله. تمثل دراسات الحالة التي ستجدها في قائمة المصادر هذه نقطة جيدة للبداية. ما الذي يعجبك على وجه التحديد في هذه المشروعات- فيما يتعلق باستخدامها لمصادر البيانات الجديدة أو الصاعدة؟ هل تستخدم أنواع البيانات الجديدة بطريقة لم ترها من قبل، أم أنها تتمكن من التوصل إلى استخلاصات جديدة بناءً على نوع جديد من التحليل؟

ابحث عن أمثلة تروق لك لمشروعات مماثلة تستخدم أنواع البيانات الجديدة بطرق معينة ترغب في تجربتها. بمجرد أن تجدها، اكتب تاريخ إنشائها، واستخرج أي عناصر تمثل إلهامًا خاصًّا لك، أو ذات صلة وثيقة بعملك. بمجرد حصولك على قائمة بالمشروعات، تواصل مع بعض الباحثين القائمين عليها لترى إذا ما كان وقتهم يسمح بإجراء مكالمة سريعة معك. تحلَّ بالواقعية: ربما يبدو أحد المشروعات في منتهى البساطة من الخارج، ولكن قد يكون تطلب عملًا أكبر مما تتخيل وراء الكواليس.

لا تتخلَّ عن النظرة الناقدة

بالرغم من الأسئلة التي تراودك، لا تزال أنت الأكثر خبرة عندما يتعلق الأمر بسياقك الخاص. إذا ما حاول أحدهم أن يخبرك بأن شيئًا ما إما أن يكون دائمًا صحيحًا أو خاطئًا على طول الخط، وتختلف معه في الرأي، فثق في حدسك.

خاصةً عندما يتعلق الأمر بالمال، فلتحصل على آراء متعددة بشأن ما يمثل خيارًا أفضل بالنسبة لك. قد لا يعطيك بائعو البرمجيات، سواء كان الربح محركهم الرئيسي أو أن نظرتهم محدودة بالتركيز على منتجاتهم الخاصة، التوصية المثلى. انظر في استخدام أدوات البرمجيات المجانية مفتوحة المصدر (FOSS) الأكثر أمنًا والأقل تكلفة في المجمل كلما أمكن ذلك.

الخاتمة

يوجد عدد من المنظمات والأفراد الذين يستخدمون هذه التقنيات لفتح آفاق جديدة أمام توثيق حقوق الإنسان بطرق حديثة وشائقة. الكثير منهم مثلوا مصادر شديدة الإلهام لهذا الدليل، ولعملنا الجماعي بشكل عام، حيث وفروا لنا لمحة مما يحدث على حدود استخدام البيانات في مجال توثيق حقوق الإنسان.

إن مجموعات مثل Forensic Architecture (فورنزيك آركيتكتشر)، قد استخدمت تقنيات مبتكرة لنمذجة البيانات في مشروعاتها لإبراز ما حدث في الماضي بناءً على معلومات محدودة بقيت بعد انتهاء الحدث؛ مثل النمذجة ثلاثية الأبعاد للبيئة المحيطة بمركب تُرك لتجرفه تيارات البحر المتوسط بعد أن لم تتحمل أي دولة مسئوليته. أصدرت المجموعة تقريرًا شكل الأساس لعدد من التظلمات القانونية الجاري التقصي عنها ضد الدول الأعضاء في حلف الناتو.

كما توجد أيضًا Bellingcat (بِلينجكات)؛ وهي شبكة من العاملين في مجال صحافة المواطن الاستقصائية، والذين يستخدمون المعلومات المتاحة علنيًّا بما يتضمن بيانات وسائل التواصل الاجتماعي، وبشكل أعم، استخبارات المصادر المفتوحة (OSINT)، للتقصي بشأن انتهاكات حقوق الإنسان وأكثر من ذلك. ساعد عمل مؤسسها إليوت هيجينز المتعلق بتقصي الهجمات الكيماوية على الغوطة بسوريا في أغسطس/ آب 2013 على إثبات أن مرتكب هذه الهجمات هو نظام بشار الأسد بشكل شبه مؤكد. وقد أصدرت الشبكة مجموعة رائعة من الموارد الإلكترونية، بما يشتمل على دراسات الحالة والدلائل التوجيهية.

استخدم الإحصائيون في مجموعة تحليل بيانات حقوق الإنسان تقنيات مبتكرة للتقييم الدقيق لضحايا الحرب في عدد من البلدان، مثل تقنية تقييم النظم المتعددة التي يعتبرون هم الرواد الأوائل في استخدامها. وكان أحد نجاحاتهم المتعددة هو إدلاء مؤسس المجموعة «باتريك بول» بشهادته في محكمة جواتيمالا العليا ضد الرئيس السابق الجنرال «خوسيه إفراين ريوس مونت»، الذي أُدين لاحقًا بارتكاب الإبادة الجماعية وجرائم ضد الإنسانية.

وبالنسبة للتحقق، فإن المنظمات والأفراد يزيدون من شفافية عملياتهم. تمكن أدوات مثل Checkdesk (تشِك دِسك) وGithub (جيت هَب) وJupyter Notebooks (جوبيتر نوتبوكس) الناس من التوثيق العلني لعملياتهم واستخلاصاتهم، بما يزيد من المصداقية ويتيح لأي شخص متابعتهم والتعلم منهم، كما أنه يفتح مجالات البحث أمام درجة جديدة من التدقيق، بما يفوق التوثيق الحقوقي الأكثر تقليدية.

إلى أين تذهب بدءًا من هنا؟

المستقبل لنا، والوقت قد حان

بين خبراتك الحقوقية والمعلومات الموجودة في هذا الدليل، لديك كل ما تحتاج إليه من أجل تقييم قيمة البيانات المختلفة بالنسبة لعملك والبدء في استخدامها.

إن الاعتبارات والتقييمات والاستخدامات المذكورة متأصلة في ممارسات تعرفها تمام المعرفة بالفعل – مثل تلك المتعلقة بالأخلاقيات والأمن والتحقق.

يظل تطوير القدرة على التقييم والفهم النقديين، لما تتيحه الأدوات والمنصات الجديدة لك وكيفية فعلها لذلك، أكثر أهمية من التركيز على أدوات بعينها. الدراية بما تفعله هذه الأدوات، وبالتحيزات المضمنة في البيانات التي تتلقاها وتعمل بها، وفوق كل ذلك التعامل المسئول مع البيانات، لا تقل أهمية عن أي وقت مضى.

في وقت صياغتك لمشروعك، قد تبدو المشروعات المذكورة عاليه أبعد ما يكون عن المتعارف عليه. وذلك لأنه بشكل عام لا يزال الباحثون الحقوقيون يستخدمون نفس التقنيات التي لطالما استخدموها على مر عقود.

سوف تستمر الزيادة فيما يتعلق بكم البيانات المتاحة وبسهولة الحصول عليها. كما ستستمر تكاليفها، مثلها مثل تكاليف كل التكنولوجيات، في الانخفاض. وبالرغم من أن منحنى التعلم قد يبدو منحدرًا في بعض الأوقات، إلا أن دمج هذه التقنيات يُعد أمرًا حيويًّا للعمل في مجال حقوق الإنسان اليوم وغدًا.

موارد وقراءات إضافية

عظّم استفادتك من الموارد والمنظمات العاملة في المجال. توفر منظمات مثل The Engine Room (ذا إنجين روم) دعمًا فنيًّا للمنظمات التي ترغب في استخدام التكنولوجيا والبيانات بصورة أكثر استراتيجية في عملها. كما أن Responsible Data community (ريسبونسيبل داتا كوميونيتي) هو مكان جيد لمن يريد الحصول على المشورة بشأن التحديات الأخلاقية أو القانونية أو تلك المتعلقة بالخصوصية، والتي تنشأ من استخدام البيانات في سياقات جديدة ومختلفة. وتوفر مجموعات مثل Tactical Technology Collective (تاكتيكال تكنولوجي كولكتيف) إرشادًا حول استخدام المعلومات من أجل المناصرة وكسب التأييد، مثل كتاب Visualising Information for Advocacy (العرض البصري للمعلومات من أجل المناصرة وكسب التأييد). وتمثل School of Data (سكول أوف داتا) موطنًا لمجتمع قوي يعمل لمساعدة مجموعات المجتمع المدني والصحفيين على استخدام البيانات لسرد الحكايات. تغطي دوراتهم الإلكترونية كل شيء بدايةً من تنظيف البيانات مرورًا بتحليلها ووصولًا إلى عرضها بصريًّا. إذا ما كنت تريد الحصول على الدعم فيما يتعلق بإنشاء قواعد البيانات واستخدامها في توثيقك، ألقِ نظرة على Benetech (بينيتك) أو HURIDOCS (هوريدوكس).

للحصول على روابط لدلائل وموارد أكثر تفصيلًا، برجاء زيارة: https://engn.it/datnav

بيانات وسائل التواصل الاجتماعي

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

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

أبحاث إعلام المواطن والتحقق:
إطار تحليلي لممارسي حقوق الإنسان

http://www.cghr.polis.cam.ac.uk/publications/cghr-practitioner-papers-series/paper-1

شهود العِيان

https://lab.witness.org

الخطوط الاسترشادية الأخلاقية لاستخدام تصوير شهود العِيان

https://lab.witness.org/announcing-witness-ethical-guidelines-for-using-eyewitness-footage-in-human-/rights

بيانات الموازنة من أجل حقوق الإنسان

مركز الحقوق الاقتصادية والاجتماعية (٢٠١٥)، الدفاع عن الكرامة: دليل لمؤسسات حقوق الإنسان بشأن رصد الحقوق الاقتصادية والاجتماعية والثقافية.

شراكة الموازنة الدولية (٢٠١٠)، دليل العمل الضريبي للمنظمات غير الحكومية.

المعونة المسيحية (٢٠١١)، مناصرة العدالة.

إلى أين تذهب بدءًا من هنا؟

شراكة الموازنة الدولية ومركز فوندار – للتحليل والتحقيق (٢٠٠٤) قيمة الكرامة دليل استخدام تحليل الميزانية لتعزيز حقوق الإنسان.

شراكة الموازنة الدولية (٢٠١٤)، المادة الثانية وموازنات الحكومات.

مفوضية الأمم المتحدة السامية لحقوق الإنسان (٢٠١٠)، حقوق الإنسان في رصد الموازنة وتحليلها ومناصرتها: دليل تدريبي.

شراكة الموازنة الدولية (٢٠٠٨)، أموالنا، مسئوليتنا: دليل المواطن لرصد الإنفاق الحكومي.

Hakikazi Catalyst (٢٠٠٦)، اتبع الأموال: دليل الموارد للمدربين بشأن تعقب الإنفاق العام في شراكة الموازنة الدولية – تنزانيا.

مؤسسة المعرفة المفتوحة، كتيب الإنفاق المفتوح، متاح على: *http://community.openspending.org/research/handbook*

موجود اليوم، مختف غدًا: الحفاظ على مقاطع الفيديو والصور على الإنترنت

أجرف أو لا أجرف
http://www.storybench.org/to-scrape-or-not-to-scrape-the-technical-and-ethical-challenges-of-collecting-data-off-the-web/

أفضل الممارسات في التجريف:
من الأخلاقيات إلى التقنيات *https://goo.gl/hovkap*
- Chilling Effects *https://lumendatabase.org*

قاعدة بيانات تجمع وتحلل الشكاوى القانونية وطلبات إزالة المواد الإلكترونية بما يتضمن مقاطع الفيديو؛ يتعاون تقرير شفافية جوجل مع هذا التوثيق بشكل مفتوح *https://www.google.com/transparencyreport/removals/copyright/faq/#chilling_effects*
- Takedown Project *http://takedownproject.org*

شريك مشروع Chilling Effects؛ جهد لتعبئة المجتمع البحثي لاستكشاف كيفية عمل إجراءات الإخطار والإزالة في الولايات المتحدة وأوروبا وبلدان أخرى، وكيفية حل هذه الإجراءات للنزاعات بين حقوق النشر وحرية التعبير.

مؤسسة التخوم الإلكترونية *https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals*

لديها دليل وأشكال بيانية مفيدة تتعلق بسياسات الإزالة لدى يوتيوب وكيفية الطعن فيها، اعرف المزيد بشأن كيفية استخدام الأقمار الصناعية للكشف عن انتهاكات حقوق الإنسان *https://www.theguardian.com/global-development-professionals-network/2016/apr/04/how-satellites-are-being-used-to-expose-human-rights-abuses*

دليل تقديمي عن الأقمار الصناعية وتحليل صور الأقمار الصناعية *http://landscape.satsummit.io*

أنشئ شريط تمرير قبل/ بعد: اختر صور الأقمار الصناعية واستضفها على الإنترنت، على فليكر مثلًا. ومن ثم انسخ وألصق الرابطين من فليكر (لا بد أن ينتهي الرابط بـ.jpg) في أداة *juxtapose https://juxtapose.knightlab.com/#create-new*

احصل على الإلهام من عدد Seeing From Above من برنامج Exposing the Invisible في تاكتيكال تكنولوجي كولكتيف، والذي يلقي الضوء على حالات التصوير الجوي في سياقات مختلفة من خلال المقابلات والتعليق والشرح *https://exposingtheinvisible.org*

دلائل متقدمة بشأن استخدام صور الأقمار الصناعية في العمل الحقوقي: رصد نزاعات الحدود باستخدام صور الأقمار الصناعية: كتيب للممارسين *http://www.aaas.org/report/monitoring-border-conflicts-satellite-imagery-handbook-practitioners,*

دليل تفسير صور الأقمار الصناعية: الحرق العمدي لأكواخ توكولز *http://hhi.harvard.edu/publications/satellite-imagery-interpretation-guide-intentional-burning-tukuls*

قوائم مرجعية للأمن الرقمي لتحديد من يمكنه الوصول إلى محتواك *https://docs.google.com/document/d/17gRphFoh7PlUrmeQNu5ADhNfty-2sEV-CLQN4Ed1hak/edit*

نظرة من أعلى: الأقمار الصناعية والطائرات بدون طيار

تصوير طائرات بدون طيار ذو صلة بحقوق الإنسان *https://www.youtube.com/playlist?list=PLRK6YeiwsEtmkkCikDM8mKSHuo9VDiE_0*

تكنولوجيات جديدة لحقوق الملكية وحقوق الإنسان والتنمية العالمية *http://drones.newamerica.org/primer/DronesAndAerialObservation.pdf*

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

طائرات بدون طيار في الاستجابة الإنسانية *https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf*

المخاطر المتعلقة بالسلامة على أرض الواقع

جمعت New Tactics for Human Rights Activism قائمة مفيدة بالاعتبارات والأدوات الخاصة بحماية العاملين في مجال حقوق الإنسان وحفاظهم على أنفسهم *https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders*

الخصوصية والمسئولية والنشاط الحقوقي *https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders*

نحو أمن شمولي للناشطين الحقوقيين *https://holistic-security.tacticaltech.org*

يحتوي حماية مصادر الصحافة في العصر الرقمي الصادر عن اليونسكو على العديد من النصائح التي تنطبق أيضًا على الباحثين الحقوقيين الذين يرغبون في حماية معارفهم *http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/Themes/Freedom_of_expression/safety_of_journalists/Protecting_Journalism_Sources_in_Digital_Age_UNESCO_Flye.pdf*

إلى أين تذهب بدءًا من هنا؟

هل أدواتك الرقمية في أمان؟

الحفظ الاحتياطي لبرمجياتك: https://securityinabox.org/en/guide/backup

الحفظ الآمن للملفات: https://securityinabox.org/en/guide/secure-file-storage

تدمير المعلومات: https://securityinabox.org/en/guide/destroy-sensitive-information

بطاقة التطبيقات الآمنة: https://www.eff.org/secure-messaging-scorecard

كتيب منتدى البيانات المسئولة لإخصائي التنمية الحديثة: https://responsibledata.io/resources/handbook/chapters/chapter-01-designing-a-project.html

إنشاء البنية التحتية للبيانات: https://responsibledata.io/resources/handbook/chapters/chapter-02-managing-data.html

مقدمة لنمذجة التهديدات https://ssd.eff.org/en/module/introduction-threat-modeling

نمذجة التهديدات للنشطاء: http://www.mobilisationlab.org/threat-modeling-for-campaigners-and-activists

دليل مؤسسة التخوم الإلكترونية للدفاع عن النفس ضد الرقابة: https://ssd.eff.org/

دليل الأمن الشمولي: https://holistic-security.tacticaltech.org

كيف تؤطر بحثك؟

مجموعة تحليل بيانات حقوق الإنسان HRDAG : المفاهيم الأساسية
https://hrdag.org/coreconcepts/

منتدى البيانات المسئولة: التعرف على الشكوك في الإحصاءات (https:// Brian Root, HRW)
responsibledata.io/reflection-stories/uncertainty-statistics/

Kelly Greenhill: إصابات نيجيريا التي لا تحصى (https://www.foreignaffairs.com/articles/africa/2015-02-09/nigerias-countless-casualties, Foreign Affairs)

جامعة طَفتس http://as.tufts.edu/politicalscience/sites/all/themes/asbase/assets/documents/newsEvents/2015febForeignAffairsGreenhill.pdf)

مطبوعات مختارة من HRDAG بشأن تحيز الاختيار
https://hrdag.org/publications/big-data-selection-bias-and-the-statistical-patterns-of-mortality-in-conflict/

تقارير توثق المنهجية البحثية المستترة في شكل قسم واحد أو عدة أقسام في تقرير:
https://hrdag.org/wp-content/uploads/201302//Gohdes_Convenience-Samples.pdf

https://hrdag.org/wp-content/uploads/201302//results-paper.pdf

https://targetedthreats.net/

https://hrdag.org/wp-content/uploads/201507//HRDAG-SY-UpdatedReportAug2014.pdf

https://hrdag.org/wp-content/uploads/201302//uv-estimates-paper_201211-.pdf

https://hrdag.org/wp-content/uploads/201302//Benetech-TRC-descriptives-final.pdf

https://hrdag.org/wp-content/uploads/201302//Benetech-Report-to-CAVR.pdf

https://hrdag.org/wp-content/uploads/201302//State-Violence-in-Chad.pdf

قبل استدعاء الخبراء... جهّز أسئلتك

مقطع فيديو:

WITNESS https://witness.org/

الطرق الإحصائية:

مجموعة تحليل بيانات حقوق الإنسان (HRDAG) *https://hrdag.org*

دمج + فهم البيانات والتكنولوجيا استراتيجيًا:

The Engine Room *https://theengineroom.org*

الجمع الآمن للبيانات + احتياجات البرمجيات // الأمن الرقمي:

Benetech *http://www.benetech.org*

إدارة الوثائق:

Huridocs *https://www.huridocs.org*

إعلام شهود العِيان: the Eyewitness Media Hub *http://www.eyewitnessmediahub.com*

Tactical Technology Collective *https://tacticaltech.org*

الشبكات/ المجتمعات New Tactics in Human Rights *https://www.newtactics.org*

شراكة الحكومة المفتوحة

http://www.opengovpartnership.org