HUMANITARIAN
LAW & POLICY

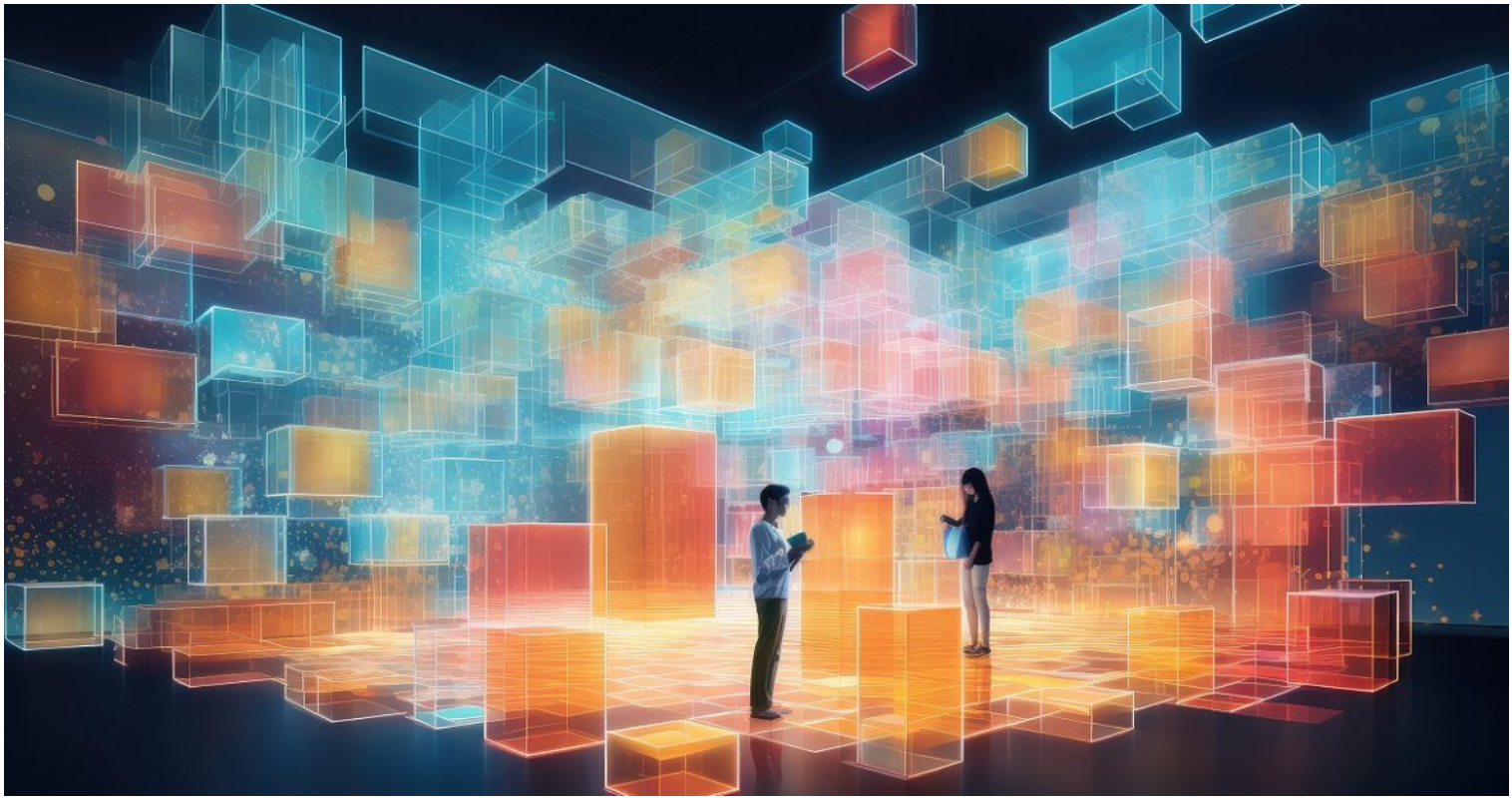
Victim/survivor-centeredness, data protection and open-source collection in accountability: lessons from IIIM-Syria

January 9, 2024, Accountability / Analysis / Artificial Intelligence and Armed Conflict / Cybersecurity and data protection in humanitarian action / Humanitarian Action / New Technologies / Technology in Humanitarian Action

9 mins read

Rayyan Ghuma
Associate Legal Officer, IIIM-Syria

Birhane Wossen Reta
Information and Evidence Officer, IIIM-Syria



The extent to which a victim/survivor-centered approach (VSCA) should be incorporated into data protection remains an emerging issue for accountability actors. What does a VSCA look like when collecting data through open-source channels, for example? On a technical level, it means having processes in place to secure and govern data. On a human level, it means recognizing the rights of victims/survivors, building trust among historically marginalized and undervalued communities, and mitigating risks to individuals whose data is entrusted to our care.

In this post, part of a new series on Cybersecurity and data protection in humanitarian action, IIIM-Syria Associate Legal Officer Rayyan Ghuma and Information and Evidence Officer Birhane Wossen Reta delve into areas of concern at the intersection of victim/survivor-centeredness, data protection, and open-source collection. They ultimately draw upon the IIIM experience to continue an ongoing conversation about data protection and the VSCA in inclusive accountability.

The conflict in Syria began over a decade ago and continues to this day. Since its inception, many actors across varying civil society sectors have worked to gather and, in some cases, publish large swaths of information relating to alleged core international crimes committed in Syria. In this context, the United Nations General Assembly, in December 2016, *established* the International, Impartial and Independent Mechanism to assist in the investigation and prosecution of persons responsible for the most serious crimes under International Law committed in the Syrian Arab Republic since March 2011 (IIIM).

The IIIM was therefore created to ensure that information and evidence of these potential crimes was safely preserved and, where appropriate, made available to competent jurisdictions for investigation and prosecution under the law. As such, although the IIIM's mandate is accountability-focused, and not humanitarian in nature, we, and by extension our accountability partners, share a similar goal with humanitarian relief organizations in that we see victims/survivors, many of whom are women and children/youth, as *active agents in their own lives*, and we set as a top priority building mutual relationships of trust.

With that in mind, very early on, the IIIM developed and integrated a *victim/survivor-centered approach* (VSCA) into every aspect of our work. Under this multifaceted rights-based approach, our success as an accountability actor has become measured, in part, by our attention to the rights of victims/survivors. When viewed through the digital lens of evidence preservation and analysis, rights-based justice requires internal processes that protect the rights—including the privacy rights—of victims/survivors throughout the data lifecycle. These internal processes should be *informed by international human rights law and internal governance frameworks*.

Privacy as a human right

The *fundamental right to a private life* has long been the starting point for data protection advocates working in accountability, and the IIIM is no exception in that regard. In fact, the UN as a whole has characterized data protection as an extension of the fundamental *right to privacy in the digital age*. The *UN Principles on Personal Data Protection and Privacy* (the Principles) are at the center of this. The Principles create an approach to processing personal data which includes, among other things, considerations of fair and legitimate processing, purpose specification, and proportionality and necessity. Internally, the UN has also signaled forthcoming regulations related to implementing data protection.

For accountability mechanisms operating within the UN, these system-wide commitments reinforce our own mandates to protect data at every stage of the data lifecycle, and especially personal data. By way of example, the IIIM categorizes a portion of the personal data it receives relating to gender and children/youth as particularly sensitive and requiring heightened security considerations when processing.*[1]* Our *Gender Strategy and Implementation Plan* therefore requires us to take steps "to ensure that sexual violence evidence…is clearly marked and effectively and confidentially tracked…" when entrusted to us. "This is important given the potential for this evidence to raise heightened privacy and protection concerns." Thus, when evaluating the fundamental rights to privacy and data protection through a VSCA, accountability mechanisms should consider the careful and secure processing of sensitive data to be at the core of our mandates.

Data protection and the IIIM mandate

In addition to looking at international human rights law and UN-specific regulations when determining an approach to data protection, we also look to our internal framework for guidance. At the IIIM, we are guided by our *mandate* and *terms of reference*. Our terms of reference dictate that we "adopt procedures and methods of work regarding…data protection, information management, case management and archiving and security issues in accordance with international criminal law standards." Our terms of reference also require that we "systematically organize all the information, documentation and evidence…such as interviews, witness testimony, documentation and forensic material, so as to ensure that their use can be maximized in…criminal investigations and prosecutions."

These obligations serve two purposes. First, they underscore the importance of handling and processing the data of victims/survivors of the conflict in Syria with the utmost care. Second, they specifically call for information governance and data protection frameworks to safeguard victim/survivor privacy and data.

Information governance in open-source collection

Much of life is represented through content published online. This is often true of conflicts as well. Although there are many factors to consider when navigating the sea of publicly available, mostly user-generated content on the internet, information governance, purpose specification and data minimization, and consent are three fundamental issues to address ahead of implementing any privacy program with an open-source component.

To start, and before a conversation on data protection can take place, we must first ensure that a baseline information governance regime is integrated into the culture of the organization. For the IIIM, this has meant implementing policies on records management, and information and cyber security, among other things. Without policies such as these in place to govern how employees handle information within an entity, the conversation about data protection compliance is not yet ripe for discussion. Therefore, even under a rights-based approach, creating an infrastructure whereby information is handled in a secure and consistent manner is a precursor to building a comprehensive privacy program. Otherwise, we are simply paying lip service to data protection. It becomes a mere formality, without any substance, and without any grit.

The second factor to address consists of the twin data protection principles of purpose specification and data minimization, the latter of which involves limiting the collection purpose to that which is necessary and relevant. What do these principles require under rights-based justice? They require answering questions about the breadth and variety of the gathered content, the collection purpose, and the overall data retention period. We, as accountability actors operating with a VSCA in mind, must embrace these questions and have processes in place to continuously re-engage them as our mandates unfold and new data comes in. Only with these principles in play can we know if we are over- or under-collecting data, and only with these principles in play can we then begin to build our data sets.

A third consideration is consent. Much has been written about the responsibilities of *humanitarian* and *human rights* organizations to obtain informed consent when collecting, storing, and processing data. Indeed, informed consent is an imperative when conducting interviews. But what does consent

entail in the context of information and evidence obtained from open-source channels, such as internet websites and social media platforms? What, for example, is an accountability mechanism's consent obligation to the uploader of a video to YouTube or the data subjects depicted in that video? These are only two of the many questions often raised in relation to consent and open-source collection. However, when it comes to data protection and the right to privacy, informed consent, even if it were possible to obtain, does not substitute for an accountability mechanism's overarching obligation to victims/survivors. Rather, under a rights-based approach to privacy, robust information governance, with all of its data protection safeguards, remains the greatest priority. Without exception, and regardless of whether consent is secured or not, accountability actors always have a responsibility to victims/survivors to consider and mitigate risks to data sources and data subjects at every stage of the data lifecycle.

In sum, accountability mechanisms face a series of challenges relating to data protection, open-source collection, and their implications for rights-based justice. When we identify and collect content from open-source channels – and when subsequent analysis enriches that content with more information about the data sources and data subjects – a VSCA mandates that we maintain its confidentiality. This requires that we quickly preserve it to prevent data loss, securely process and store it to mitigate risk of breach, and selectively and responsibly share it with prosecuting jurisdictions. The IIIM takes this mandate and corresponding responsibilities under the VSCA very seriously. We see each of them as *pivotal to achieving longer term, comprehensive, and inclusive accountability* for core international crimes committed in Syria. Victims/survivors of the conflict in Syria deserve nothing less.

[1] Personal data is that data which relates to an identified or identifiable natural person. Sensitive personal data is a subset of personal data that relates to racial or ethnic origin; political, religious or philosophical opinions or beliefs; trade union membership; genetic or biometric data processed to uniquely identify a person; and/or data concerning a person's health; sex life; or sexual orientation. Data protection seeks to protect personal data, including sensitive personal data, from unauthorized processing.

See also:

- Megan O'Brien, *Online violence: real life impacts on women and girls in humanitarian settings*, January 4, 2024
- Roxana Radu, Eugenia Olliaro, *Not child's play: protecting children's data in humanitarian AI ecosystems*, December 14, 2023
- Susanna Acland, Barnaby Willitts-King, *Mobile phones for participation: building responsible public-private humanitarian partnerships*, December 7, 2023
- Ed Millet, *Deploying OSINT in armed conflict settings: law, ethics, and the need for a new theory of harm*, December 5, 2023

Tags: armed conflict, cybersecurity, data protection, humanitarian action, osint, survivors, Syria, victims, vsca

You may also be interested in:

Online violence: real life impacts on women and girls in humanitarian settings

11 mins read

Accountability / Analysis / Artificial Intelligence and Armed Conflict / Cybersecurity and data protection in humanitarian action / Humanitarian Action / New Technologies / Technology in Humanitarian Action

Megan O'Brien

Online violence is not contained by the digital sphere – it is killing women and ...

Israel and the occupied territories: how international humanitarian law applies

18 mins read

Accountability / Analysis / Artificial Intelligence and Armed Conflict / Cybersecurity and data protection in humanitarian action / Humanitarian Action / New Technologies / Technology in Humanitarian Action

Cordula Droege & Elizabeth Rushing

Since the 7th of October, the world has witnessed a new and unimaginable wave of ...