

The struggle against sexual violence in conflict: Investigating the digital turn

Kristin Bergtora Sandvik and Kjersti Lohne*

Kristin Bergtora Sandvik (SJD, Harvard Law School, 2008) is a Professor of Legal Sociology at the Faculty of Law, University of Oslo, and a Research Professor in Humanitarian Studies at the Peace Research Institute Oslo (PRIO). Her work focuses on refugee resettlement, legal mobilization, humanitarian technology, ethics, innovation and accountability.

Kjersti Lohne is a Postdoctoral Researcher at the Faculty of Law, University of Oslo. Her work focuses on the sociology of international law, international criminal justice, human rights advocacy and transnational networks.

Abstract

Digital technological innovations make new types of responses to conflict-related sexual violence (CRSV) possible, bringing with them both potential promises and pitfalls. Aiming to provide a conceptual starting point for further analysis, this article problematizes the trend towards data extraction in exchange for aid, protection and justice, and argues for the importance of complementing technology-driven approaches to the struggle against CRSV with the inclusion of strategies for user participation and investment in digital literacy as key aspects of the response. To explore how the digital turn shapes the struggle against CRSV, the article offers a three-part analytical framework. First, the article unpacks how digital technologies create corresponding “digital bodies” – comprised of images,

* Research for this paper was funded by the PRIO-hosted project “Do No Harm: Ethical Humanitarian Innovation” and the University of Oslo-hosted project “Vulnerability in the Robot Society”, both funded by the Research Council of Norway.

information, biometrics and other data stored in digital space – which represent the bodies of individuals affected by sexual violence, and which interplay with the risks posed upon the physical bodies of those facing CRSV. Second, the article maps out the role of digital technologies in a cycle of intervention, including prevention of, response to, documentation of and accountability for CRSV. Third, recognizing the increasing importance of data governance to the struggle against CRSV, the article considers how divergent humanitarian, human rights and international criminal law approaches to data may create different pathways for CRSV data. This could also give rise to new tensions in how international actors approach CRSV.

Keywords: conflict-related sexual violence, digital bodies, digital literacy, humanitarian data, sexual violence, human rights, international criminal justice.

⋮⋮⋮⋮⋮

Introduction

Historically, the cultural stigma of rape and the international community's long-standing disregard of conflict-related sexual violence (CRSV) have meant that little was known about this form of violence. Currently, CRSV actors – from field responders to international judges – have more than sufficient information regarding the occurrence of CRSV: they are overwhelmed by it and need tools for sorting, identifying and analyzing actionable data and viable paths for action.¹ As a result of global connectivity and the affordability and mass distribution of digital devices, new types of responses to CRSV are now possible. Increasingly, digital technological innovations such as humanitarian mega-databases, or “superplatforms”,² are harvesting and registering data on a mass scale. Yet, this trend towards the extraction of data from vulnerable individuals in exchange for protection, aid and justice also confronts the struggle against CRSV with new dilemmas. Moreover, CRSV actors must find ways to respond effectively to the proliferation of digital technology-based threats.

- 1 Elisabeth Jean Wood, “Conflict-Related Sexual Violence and the Policy Implications of Recent Research”, *International Review of the Red Cross*, Vol. 96, No. 894, 2014; Carlo Koos, “Sexual Violence in Armed Conflicts: Research Progress and Remaining Gaps”, *Third World Quarterly*, Vol. 38, No. 9, 2017; Jelke Boesten and Marsha Henry, “Between Fatigue and Silence: The Challenges of Conducting Research on Sexual Violence in Conflict”, *Social Politics: International Studies in Gender, State, and Society*, Vol. 25, No. 4, 2018; Anette Bringedal Houge, “Sexualized War Violence: Knowledge Construction and Knowledge Gaps”, *Aggression and Violent Behavior*, Vol. 25, 2015.
- 2 “Superplatforms”, or “platforms of platforms”, are giant internet companies that operate across multiple sectors, such as Apple, Facebook, and Google. See, for example, David Porteous and Olga Morawczynski, “The Superplatforms are Coming ... and They Will Transform Financial Inclusion”, *NextBillion*, 21 December 2018, available at: <https://nextbillion.net/the-superplatforms-are-coming-and-they-will-transform-financial-inclusion/> (all internet references were accessed in January 2021). We use this term for the emergence of platforms such as the Office of the UN High Commissioner for Refugees' (UNHCR) PRIMES (see: www.unhcr.org/primes.html) and the World Food Programme's SCOPE (see: <https://tinyurl.com/y4axb5br>).

Despite considerable interest in and abundant literature on CRSV,³ there is a dearth of critical research and reflection on the ability of digital technologies to assist in the struggle against it. This article suggests cautious optimism regarding the potential role and relevance of digital technology in preventing, mitigating, treating and punishing CRSV. While we advise against seeing digital technology as a panacea, we emphasize the importance of thinking carefully through the potential for improvements and positive change. The contribution of the article is to offer an analytical framework for assessing the role and relevance of digital technologies, broadly defined as digital devices and data, in addressing CRSV. Our analytical framework has three main components:

1. Digital technologies interact with the insecure and unstable context of conflicts in ways that may produce and exacerbate risk and harm. CRSV actors need a better grasp of how this happens and what this means for the struggle against CRSV. To that end, we introduce the notion of “digital bodies” as a cross-cutting analytical concept to better understand how technologization may also engender risk and harm.⁴ Digital technologies are a fundamental part of the contemporary experience and re-conceptualization of the body. At the same time, in conflict-ridden and fragile settings, the provision of data about the body is increasingly a precondition for receiving services, legal protection and justice from the international community. To that end, “digital bodies” as an analytical concept enables cross-sectoral conversations about power and responsibility. Understanding the nature of risk for women’s physical bodies as well as women’s digital bodies, and the interplay between the two—but also the potential for activism and participation—is crucial for understanding the role and relevance of digital technology in grappling with CRSV. The point is not that women’s digital and physical bodies are the same, but that compromising or neglecting the security of digital bodies may be *as consequential* as compromising the security and well-being of physical bodies.
2. We classify and identify digital technological trends and problem framings in the CRSV field through the introduction of a “cycle of intervention”, where we assess the digital transformation of the struggle against CRSV in the fields of prevention, response, documentation and accountability. The cycle follows a set of transnational continuums: from the conflict setting to international institutions and global data brokers, and from the prevention stage to the justice and accountability phase, taking place long after the violent event.
3. Recognizing the importance of how data collection, storage, sharing, aggregation and use shape all phases of the struggle against CRSV, we reflect on how divergent perspectives on data may shape the pathways of CRSV data. The article compares and contrasts humanitarian, human rights and

3 See also the thematic issue of the *Review* on “Sexual Violence in Armed Conflict”, Vol. 96, No. 894, 2015, available at: <https://international-review.icrc.org/reviews/irrc-no-894-sexual-violence-armed-conflict>.

4 We understand technologization as the incremental development and application of technology-based approaches.

international criminal justice approaches to data in order to illustrate how new dilemmas may arise with respect to the management and sharing of CRSV data. By looking at the different sectors' objectives, time frames, and perceived agency of those targeted for intervention, we reflect on how the objectives, approaches and values of the three sectors may complement each other, but also create new frictions in the context of the digital turn.

For the purposes of this article, we rely broadly on the United Nations (UN) conceptualization of the term “conflict-related sexual violence” as referring to “rape, sexual slavery, forced prostitution, forced pregnancy, forced abortion, enforced sterilization, forced marriage, and any other form of sexual violence of comparable gravity perpetrated against women, men, girls or boys that is directly or indirectly linked to a conflict”.⁵ While the article generally addresses all categories of victims/survivors listed in this definition, the analytical focus of the article and the empirical and scholarly contributions on which it draws are largely concerned with the experiences of women. As noted above, so far little attention has been given to digital technologies and CRSV. Thus, to develop a comprehensive conceptual framework for further analysis, the article draws on scholarly and grey literature and media reports on how technology is used to address sexual violence also in non-conflict settings.⁶ Acknowledging the resulting partial scope of the article, we hope that it may serve as a resource for others working to plug important knowledge gaps.

The article proceeds in three main parts. In laying out the first part of our analytical framework, we offer a conceptualization of digital bodies. This includes a brief account of how digital technologies transform dynamics of conflict, crisis and injustice, but also constitute a potential for change. We also situate the digital body in a potentially powerful *moral economy* emerging from the digital turn, and the political economy generated by the fight against CRSV.⁷ The second component of the analytical framework helps us illustrate how digital technologies shape different aspects of the struggle against CRSV. We introduce a “cycle of intervention”, mapping out initiatives involving the use of digital technologies to prevent, provide treatment for, investigate and enhance criminal accountability for sexual violence. For the third part of the analytical framework, we provide a typology for understanding the nature and implications of different perspectives on data in the fields of humanitarian aid, human rights practice and international

5 António Guterres, *Conflict-Related Sexual Violence: Report of the United Nations Secretary-General*, UN Doc. S/2019/280, 29 March 2019, available at: https://peacekeeping.un.org/sites/default/files/annual_report_of_the_sg_on_crsv_2018.pdf.

6 To that end, the article builds on and develops insights from Kristin Bergtora Sandvik, *Technologizing the Fight against Sexual Violence: A Critical Scoping*, PRIO Working Paper, Oslo, 2019, available at: <https://gps.prio.org/Publications/Publication/?x=1274>; Kristin Bergtora Sandvik, “Digital Dead Body Management (DDBM): Time to Think it Through”, *Journal of Human Rights Practice*, Vol. 12, No. 2, 2020, available at: <https://doi.org/10.1093/jhuman/huaa002>.

7 While the notion of moral economy is used to describe those norms and habits embedded in market rationalities, more broadly it is also concerned with what it is that lends legitimacy to the constitution of markets and the economy. See Susanne Karstedt and Stephen Farrall, “The Moral Economy of Everyday Crime: Markets, Consumers and Citizens”, *British Journal of Criminology*, Vol. 46, No. 6, 2006.

criminal justice. We conclude by re-emphasizing the importance of digital literacy and participation in the struggle against CRSV. Our conceptualization of digital literacy is a critical one: it includes not only the capacity to use a device and understand the basic purpose of using it, but also having a basic grasp of issues of law, digital risk and rights, and an awareness of what it means to have a digital body—that is, a body made legible as data. Digital literacy thus goes beyond technical competence to include awareness and perceptions about technology, law, rights and risk.

Re-conceptualizing security through digital bodies

Whether in peace or war, digital technology is a fundamental part of the contemporary experience and re-conceptualization of the body. Via technological means, there is an “intensification of the extension, abstraction, and reconstruction”⁸ of the body. The first aspect of our analytical framework concerns how the use of digital technologies creates corresponding “digital bodies”—i.e., images, information, biometrics and other data stored in digital space—that represent the physical bodies of individuals affected by sexual violence, but over which they have little say or control. Understanding this double risk—for the physical body as well as the digital body, and the interplay between the two—is crucial for properly gauging the role and relevance of digital technology in the struggle against CRSV.⁹ We argue that the digital body should also be a separate point of departure for security considerations.

Early cultural approaches to the study of cyborgs explored how “digital bodies” operated in the discourses of digital culture to refer to those avatars and images that represented and simulated humans on-screen.¹⁰ While these digital bodies were tropes in popular culture in the 1980s and 1990s, technological innovation has increasingly given them a presence in everyday life. Haggerty and Erickson describe how “surveillant assemblages” operate by abstracting human bodies from their territorial settings and separating them into a series of different flows, to be reassembled in different locations as discrete and virtual “data doubles”, which can be scrutinized and targeted for intervention.¹¹ In this way,

- 8 Chris Shilling, “The Body in Sociology”, in Claudia Malacrida and Jacqueline Low (eds), *Sociology of the Body*, Oxford: Oxford University Press, 2008; Carey Jewitt, Sara Price and Anna Xambo Sedo, “Conceptualising and Researching the Body in Digital Contexts: Towards New Methodological Conversations across the Arts and Social Sciences”, *Qualitative research*, Vol. 17, No. 1, 2017.
- 9 See K. B. Sandvik, *Technologizing the Fight against Sexual Violence*, above note 6. See also Kristin Bergtora Sandvik, “Making Wearables in Aid: Digital Bodies, Data and Gifts”, *Journal of Humanitarian Affairs*, Vol. 1, No. 3, 2019; Kristin Bergtora Sandvik, “Wearables for Something Good: Aid, Dataveillance and the Production of Children’s Digital Bodies”, *Information, Communication & Society*, Vol. 23, No. 14, 2020.
- 10 Donna Haraway, “Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s”, *Socialist Review*, No. 80, 1985. A cyborg is a person whose physiological functioning is aided by or dependent upon a mechanical or electronic device; see: www.dictionary.com/browse/cyborg.
- 11 Kevin D. Haggerty and Richard V. Ericson, “The Surveillant Assemblage”, *British Journal of Sociology*, Vol. 51, No. 4, 2000.

translating human identity into information patterns not only provides more information, it also creates new conceptions of identity. The body itself becomes the source of information – the coded body can “talk”. As illustrated by scholarly analysis of migration management, this may imply that “a talking individual, who owns the body, is in fact seen as unnecessary” and, more importantly, may be considered insufficient and even suspect as a source of identification, as the coded body is considered more “truthful”.¹²

Much of the literature investigating the *gendered* dimensions of the digital body takes as its starting point the social nature of the body, and is concerned with contestations over sex/gender/nature/culture, and the bodywork undertaken to forge links between physical and virtual bodies.¹³ As with the broader feminist discourse on anti-essentialism,¹⁴ there is little agreement about what a body is. However, with increasing technologization, attention must be paid to how digital technologies have become instruments facilitating the making of truth claims about the body.¹⁵ In the context of CRSV, this concerns what happened when, to whom, by whom and how. While digital technologies offer novel ways of constructing and communicating about gender, gender roles and gendered violence, they also bring the possibility of new modes of disempowerment and abuse, with implications for real-life sexual violence.¹⁶

It is important to reiterate that for the CRSV context, the digital body is not a metaphysical concept. In conflict-ridden and fragile settings, it is common practice for underserved, abandoned and structurally discriminated-against communities to be called upon to provide data as a precondition for receiving services, legal protection and justice in the form of legal accountability, truth and reparations.¹⁷ Whereas technology actors and States engage in heavy dataveillance of consumers/citizens,¹⁸ the extra-democratic governance structures of the international community and the vulnerability of individuals and communities in crisis magnify the power exercised over such communities and exacerbate existing

- 12 Katja Franko Aas, “‘The Body Does not Lie’: Identity, Risk and Trust in Technoculture”, *Crime, Media, Culture*, Vol. 2, No. 2, 2006.
- 13 Kate O’Riordan, “Revisiting Digital Technologies: Envisioning Biodigital Bodies”, *Communications*, Vol. 36, No. 3, 2011.
- 14 Candace West and Don H. Zimmerman, “Doing Gender”, *Gender & Society*, Vol. 1, No. 2, 1987.
- 15 Theresa M. Senft, “Introduction: Performing the Digital Body – a Ghost Story”, *Women & Performance: A Journal of Feminist Theory*, Vol. 9, No. 1, 1996, available at: <https://tinyurl.com/y3nmjhmq>; Breanne Fahs and Michelle Gohr, “Superpatriarchy Meets Cyberfeminism: Facebook, Online Gaming, and the New Social Genocide”, *MP: An Online Feminist Journal*, Vol. 3, No. 6, 2010.
- 16 See Ian Sample, “Internet ‘Is not Working for Women and Girls’, Says Berners-Lee”, *The Guardian*, 12 March 2020, available at: www.theguardian.com/global/2020/mar/12/internet-not-working-women-girls-tim-berners-lee.
- 17 Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, “Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation”, *International Review of the Red Cross*, Vol. 99, No. 904, 2017; Mirca Madianou, “Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises”, *Social Media + Society*, Vol. 5, No. 3, 2019.
- 18 Dataveillance is the systematic monitoring of people or groups by means of personal data systems in order to regulate or govern their behaviour. Sara Degli Esposti, “When Big Data Meets Dataveillance: The Hidden Side of Analytics”, *Surveillance & Society*, Vol. 12, No. 2, 2014, available at: <https://doi.org/10.24908/ss.v12i2.5113>.

power differences between organizations (with their private sector partners), on the one hand, and communities in crisis, on the other. Increasingly, this form of governance centres on extracting data in exchange for aid, protection and justice.¹⁹ In what follows, we explore the nature of risk for women’s physical and digital bodies posed by digital transformations—but also the potential for activism and participation—as a means to start analyzing the role and relevance of digital technologies in the struggle against CRSV.

Digital transformations, harms, solution(ism)s and change

For those seeking to remedy harm in conflict settings, the availability and use of mobile phones, social media platforms, satellites, drones, digital cash and biometric technology have transformed how human suffering is identified, registered, understood and addressed, by whom, and from where.²⁰ At the same time, the opportunities provided by technological developments exacerbate gendered risks²¹ and harms and produce new ones.²² The sophistication and affordability of off-the-shelf commercial devices enable intimate surveillance and the production of false information and fake imagery—i.e., false digital bodies. For example, “deepfake” pornographic videos of Chandrani Murmu, Indian’s youngest parliamentarian, were circulated as part of the widespread “trolling” and online sexual harassment of India’s female politicians.²³

Moreover, digital technologies also shape the way in which individuals experience violence. Global connectivity extends the reach of offenders and deprives victims/survivors of privacy by facilitating access to information, providing private ways to communicate, preserving images of assaults, and making anonymous harassment possible. Over the last ten to fifteen years, it has been increasingly recognized that “technology-related forms of violence against women cause psychological and emotional harm, reinforce prejudice, damage reputation, cause economic loss and pose barriers to participation in public

19 K. B. Sandvik, “Wearables for Something Good”, above note 9.

20 See K. B. Sandvik, “Making Wearables in Aid”, above note 9; Kristin Bergtora Sandvik, Maria Gabrielsen Jumbert, John Karlsrud and Mareile Kaufmann, “Humanitarian Technology: A Critical Research Agenda”, *International Review of the Red Cross*, Vol. 96, No. 893, 2014; K. B. Sandvik, K. L. Jacobsen and S. M. McDonald, above note 17. See also special issue of the *International Journal of Transitional Justice* on “Technology and Transitional Justice”, Vol. 13, No. 1, 2019.

21 For an exploration of the gendered aspects of risk—that is, how risk shapes the lives of different genders because of their gender—see Kelly Hannah-Moffat and Pat O’Malley (eds), *Gendered risks*, Routledge-Cavendish, London and New York, 2007.

22 We also note the risk that digital technology reproduces biases and discrimination in society and in data sets. For example, if the working assumption is that CRSV only affects women and girls, then men, boys, and sexual and gender minority individuals will remain invisible. For an analysis of two examples of algorithmic exclusion of men and boys—in the UNHCR’s vulnerability assessments and in drone strikes—see Kristin Bergtora Sandvik, “Technology, Dead Male Bodies, and Feminist Recognition: Gendering ICT Harm Theory”, *Australian Feminist Law Journal*, Vol. 44, No. 1, 2018.

23 See Eliza Mackintosh and Swati Gupta, “Troll Armies, ‘Deepfake’ Porn Videos and Violent Threats: How Twitter Became So Toxic for India’s Women Politicians”, CNN, available at: <https://edition.cnn.com/2020/01/22/india/india-women-politicians-trolling-amnesty-asequals-intl/index.html>.

life”.²⁴ Nevertheless, there is little reporting of or response to the intersections of CRSV and digital technologies, and the way risk and harm are evolving is insufficiently understood, particularly in the international domain.²⁵ Our use of the concept of digital bodies aims to make visible both the multiple emergent forms of CRSV risk and the need for interventions to address the protection needs of this “double” body – both physical and digital.

Digital technologies are also significantly shaping the potential to mitigate and respond to conflicts and other situations of violence. Technology provides tools for victims/survivors and those who work with them or on their behalf. Digital devices and platforms can give victims/survivors therapeutic space by enabling them to receive assistance, speak out, share their stories, and gain recognition of harm and trauma, thus offering possibilities for social change.²⁶ At the same time, we underline the importance of giving due consideration to digital literacy and the digital body in designing interventions.

Due to the scarcity of analysis on the use of digital technologies in the struggle against CRSV, we here briefly note the mushrooming of initiatives offering digital technology-based solutions to sexual violence in non-conflict settings: these include digital platforms and blockchain technologies designed to raise awareness, advocate for change and offer possibilities for protection, reporting and the crowdsourcing of justice. Such initiatives have been animated by the #MeToo campaign and its interweaving of feminist consciousness – an awareness of women’s inequality and a commitment to remedy it – and Silicon Valley solutionism – recognizing “problems as problems based on just one criterion: whether they are ‘solvable’ with a nice and clean technological solution”.²⁷ We have seen, for example, the emergence of sophisticated legal technology dealing with sexual violence, such as Callisto, a blockchain-based matching system that allows survivors to share their stories and securely connects victims of the same perpetrator to identify repeat offenders,²⁸ and LegalFling, a platform for uploading consent to sexual activity.²⁹

From a CRSV perspective, these approaches may appear to abstract the issue of sexual violence from its systemic context. Access to digital devices is assumed, as is a focus on individual agency and generally high levels of digital

24 Katerina Fialova and Flavia Fascendini, *Voices from Digital Spaces: Technology-Related Violence against Women*, Association for Progressive Communications, 2011; Archana Barua and Ananya Barua, “Gendering the Digital Body: Women and Computers”, *AI & Society*, Vol. 27, No. 4, 2012; Rhonda Shaw, “‘Our Bodies, Ourselves’, Technology, and Questions of Ethics: Cyberfeminism and the Lived Body”, *Australian Feminist Studies*, Vol. 18, No. 40, 2003.

25 But see Dubravka Šimonović, *Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective*, UN Doc. A/HRC/38/47, 18 June 2018, available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/47.

26 See, for example, “Sexual Assault and Technology Misuse”, *VAWnet*, available at: <https://vawnet.org/events/sexual-assault-and-technology-misuse>.

27 Evgeny Morozov, “The Perils of Perfection”, *New York Times*, 2 March 2013, available at: www.nytimes.com/2013/03/03/opinion/sunday/the-perils-of-perfection.html; see also Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, PublicAffairs, New York, 2013.

28 See the Callisto website, available at: www.projectcallisto.org.

29 See the LegalFling website, available at: <https://legalfling.io/>.

literacy – and the problem and solution are both “produced” in the global North. However, we suggest that they are also examples of serious attempts to rethink the gender-based and sexual violence equation, offer visibility, build feminist consciousness and strengthen advocacy in new ways.³⁰ As such, these innovations are a starting point, not an end point, for thinking about the use of digital tools in the struggle against CRSV.

Moral economies and the power of problem framing

Furthermore, we must consider the power of problem framing as two contemporary trends intersect. Across the humanitarian, human rights and international criminal justice sectors, the use of digital technologies is gaining traction as a way to make service delivery, truth, accountability and justice more efficient and cheaper.³¹ This faith in technology is supported by a burgeoning “ICT for good” literature making optimistic claims about the capacity of technology to solve political and social issues.³² In parallel, a political economy of sexual violence has emerged whereby the moral, political, legal and financial attention given to CRSV risks crowding out agency, participation and recognition of the continuum of violence affecting women in conflict, which includes but is not limited to sexual violence.³³ While acknowledging the plethora of different policies and tools developed by international, State and non-State organizations alike to prevent CRSV, there is concern that the contemporary and dominant focus on sexual violence may sideline alternative framings with respect to women’s insecurity.³⁴

Without undermining the attention that CRSV (finally) elicits, the converging interests among activists, academics and politicians – as concerns both the focus on digital technologies and CRSV – should give pause for thought. Especially, difficult questions should be asked about the potential for a powerful moral economy of the technologized struggle against CRSV: who frames problems and solutions when it comes to CRSV, and what are the direct and indirect burdens of this framing? As well, who benefits from the assumption that digital technologies will facilitate the struggle against CRSV, and why? What does it mean for how we calibrate the vulnerability – and utility – of digital bodies in

30 See Doreen Raheena Sulleyman, “Sexual Assault in Ghana: How Technology Can Help Build Visibility”, *GenderIT.org*, 6 February 2019, available at: www.genderit.org/feminist-talk/sexual-assault-ghana-how-technology-can-help-build-visibility.

31 Kristin B. Sandvik and Kjersti Lohne, “The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept”, *Millennium*, Vol. 43, No. 1, 2014.

32 Patrick Meier, “New Information Technologies and Their Impact on the Humanitarian Sector”, *International Review of the Red Cross*, Vol. 93, No. 884, 2011. For a discussion of this literature, see Kristin Bergtora Sandvik, “Now Is the Time to Deliver: Looking for Humanitarian Innovation’s Theory of Change”, *Journal of International Humanitarian Action*, Vol. 2, No. 1, 2017, p. 8.

33 Paul Kirby and Laura J. Shepherd, “The Futures Past of the Women, Peace and Security Agenda”, *International Affairs*, Vol. 92, No. 2, 2016. See also Maria Eriksson Baaz and Maria Stern, *Sexual Violence as a Weapon of War? Perceptions, Prescriptions, Problems in the Congo and Beyond*, Zed Books, London and New York, 2013.

34 See also Anette Bringedal Houge and Kjersti Lohne, “End Impunity! Reducing Conflict-Related Sexual Violence to a Problem of Law”, *Law & Society Review*, Vol. 51, No. 4, 2017.

the CRSV context? To scope the range of possibilities and provide a shared frame of reference for critical discussion, the next section maps a cycle of digital technological intervention to CRSV.

Digital technologies and CRSV: Mapping a cycle of intervention

The second part of our analytical framework provides an analytical approach to classifying and identifying digital technological trends and problem framings in the CRSV field. We map a cycle of digital technological interventions, where gadget distribution and acceptance combine with strategies for large-scale data harvesting and effective data management. The cycle is mapped onto a transnational continuum from the conflict setting to international institutions and global data brokers, and from the preventive phase to efforts to obtain justice and accountability occurring long after the violence.

Prevention

An important insight emerging from the last two decades of analysis of CRSV is that sexual violence is not necessarily random, unplanned and unforeseeable, but is often preceded by rumour and hate speech, sudden or irregular troop movements, the separation of men and women at checkpoints and so forth.³⁵ Early warning is therefore key for preventing sexual violence, and digital technologies can be an essential element of this response. In particular, data-driven predictive approaches have significant potential in contexts where connectivity, mobile phone ownership and social media use are widespread. This includes prediction based on the analysis of big data sets,³⁶ the identification of sites of sexual violence and harassment,³⁷ and the use of automated detection based on machine learning and natural language processing to identify patterns of hate speech and rumour in social media that dehumanize and sexualize particular groups or individuals. Satellite surveillance footage and drone imagery can also help map physical movements and actions and identify indicators of heightened risk of sexual violence.³⁸

At the same time, technology-driven early-warning initiatives raise difficult questions about operability, relevance and risk. At a technical level, there will always be issues related to algorithmic bias, access to relevant local data traffic, and

35 E. J. Wood, above note 1. See also António Guterres, *Report of the Secretary-General on Conflict-Related Sexual Violence*, 16 April 2018, available at: www.un.org/sexualviolenceinconflict/wp-content/uploads/reports/sg-reports/SG-REPORT-2017-CRSV-SPREAD.pdf.

36 Dara Kay Cohen and Ragnhild Nordås, "Do States Delegate Shameful Violence to Militias? Patterns of Sexual Violence in Recent Armed Conflicts", *Journal of Conflict Resolution*, Vol. 59, No. 5, 2015.

37 Chelsea Young, "HarassMap: Using Crowdsourced Data to Map Sexual Harassment in Egypt", *Technology Innovation Management Review*, Vol. 4, No. 3, 2014.

38 Joshua Lyons "Documenting Violations of International Humanitarian Law from Space: A Critical Review of Geospatial Analysis of Satellite Imagery during Armed Conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009)", *International Review of the Red Cross*, Vol. 97, No. 866, 2012.

adequate local knowledge and translation capacity. Aerial surveillance is useful only if timely and of high quality, and where enough imagery analysis capacity is available. Satellites are expensive, and drones require significant local infrastructure. Moreover, surveillance is not necessarily predictive: the violence may already be ongoing. Neither is it active: knowing about atrocities is not the same as acting on them, and there is no necessary causal link between remote monitoring and protection efforts being implemented on the ground. Similarly, the assumption that there is a causal relationship between early warning and self-rescue is problematic. For example, distributing free phones to women at risk is a fairly common strategy. However, in addition to possibly revealing the whereabouts of their users, phones may get lost or be confiscated, or may not work, and they may also create a dynamic whereby women are (inherently) put under pressure to “produce cases” in order to prove efficacy. In addition, the notion of data having an inherent protective effect is based on the assumption that increased amounts of unique and otherwise unobtainable data over wide geographic areas and/or non-permissive environments result in targeted communities having an early warning, which enables them to make better and quicker decisions that are potentially life-saving.³⁹

The impact of this type of early-warning system – whether organized by external actors or community-based – will also depend on trust in technology and in the message itself. Over the last two decades, digital technologies have been used for awareness-raising, consciousness-raising, training and capacity-building. For grassroots and community-based actors, they are used to document and disseminate information about harms and threats, create digital support networks, give early warnings and trigger support from powerful constituents.⁴⁰ Yet in this regard, digital technologies occupy an ambiguous position. On the one hand, for activists, technology produces indisputable “facts”, testimonies, or evidence of events in formats familiar and acceptable to those in power. Even if the physical body cannot speak with credibility – for example, when we take into account that refugee narratives are often met with distrust⁴¹ – digital devices are seen as credible conveyors of information.

On the other hand, in recent years, countering misinformation (false information not created to do harm), disinformation (false information created to do harm) and malinformation (“true” information used to inflict harm) has become increasingly complicated.⁴² In the past, the aim was to harness the power

39 Kristin Bergtora Sandvik and Nathaniel Raymond, “Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response”, *Genocide Studies and Prevention: An International Journal*, Vol. 11, No. 1, 2017.

40 Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018.

41 Kristin Bergtora Sandvik, “The Physicality of Legal Consciousness: Suffering and the Production of Credibility in Refugee Resettlement”, in Richard D. Brown and Richard Ashby Wilson (eds), *Humanitarianism and Suffering: The Mobilization of Empathy*, Cambridge University Press, Cambridge, 2008.

42 Council of Europe, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, 2017, available at: www.coe.int/en/web/freedom-expression/information-disorder.

of social media to do good, but social media is now also seen as a source of harm.⁴³ The rise of deepfake images/videos and generative adversarial networks⁴⁴ poses particular problems for early warning. For example, rumours about rapes and child killings usually trigger acts of revenge. Graphical illustrations of such crimes can prove fatal, regardless of whether or not they are verifiable. False attribution of imagery producing false digital bodies –such as a deepfake app generating nude images of women⁴⁵ – exacerbates vulnerability.

All these factors dovetail with more general issues related to cyber security and the use by governments and armed non-State actors of surveillance, kill switches and offensive cyber weapons. We therefore urgently need early-warning approaches that will identify hate speech and rumours, produce evidence that they are untrue and, in culturally meaningful ways, rapidly disseminate counter-messages to diffuse potential violence.⁴⁶ At the same time, it seems clear that the future of early warning depends on participatory approaches, such as training and capacity-building designed to enhance user competence. Most importantly, increased attention to digital literacy in early-warning approaches will enable communities to gauge the scope of digital manipulation, undertake value assessments about the kind of sexual violence produced by digital devices and the type of gendered harm it causes, and make realistic risk assessments.

Response

There are many examples of how digital technologies are helping activists to self-protect and to organize community protection. For example, crowdsourcing approaches provide documentation of locations and stories of assault,⁴⁷ and apps send the times and GPS coordinates of arrests to families, fellow activists, legal advisers and social media outlets.⁴⁸ These technologies can also offer individuals at risk and survivors of sexual violence access to services when there is stigma and generalized insecurity, and can help field responders to achieve a greater degree of internal coordination and coherence and to avoid duplication of

43 Sam Gregory, “Cameras Everywhere Revisited: How Digital Technologies and Social Media Aid and Inhibit Human Rights Documentation and Advocacy”, *Journal of Human Rights Practice*, Vol. 11, No. 2, 2019.

44 See Joseph Rocca, “Understanding Generative Adversarial Networks”, *Towards Data Science*, 7 January 2019, available at: <https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29>.

45 See James Vincent, “New AI Deepfake App Creates Nude Images of Women in Seconds”, *The Verge*, 27 June 2019, available at: www.theverge.com/2019/6/27/18760896/deepfake-nude-ai-app-women-deepnude-non-consensual-pornography.

46 On the trade-offs between freedom of speech and security, as well as the risks inherent in limiting freedom of speech, see David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/74/486, 9 October 2019, available at: www.ohchr.org/Documents/Issues/Opinion/A_74_486.pdf.

47 See Anastasia Powell and Tully O’Neill, “Cyber Justice: How Technology is Supporting Victim-Survivors of Rape”, *The Conversation*, 5 April 2016, available at: <https://theconversation.com/cyber-justice-how-technology-is-supporting-victim-survivors-of-rape-56022>.

48 Sheila Peuchaud, “Social Media Activism and Egyptians’ Use of Social Media to Combat Sexual Violence: An HiAP Case Study”, *Health Promotion International*, Vol. 29, No. 1, 2014.

services and victim interviewing. Digital technologies can provide gender-sensitive screening tools, and training platforms for field responders. Digital screening tools are being developed, along with multiple tools for navigating services and accessing information safely: so-called digital “safe spaces”.⁴⁹ And while record-keeping in conflict and fragile contexts is challenging, digitized health records are less likely to be lost or destroyed, as long as the integrity of the database is intact.

Ideally, digital technologies can be used to better safeguard patients’ physical security and confidentiality. For therapeutic interventions to be effective, accessible information about the nature and function of particular treatments is crucial, and digital technologies can provide this information. In settings with few resources, there is an acute shortage of mental health professionals; in such contexts, Internet-based interventions, text messaging, and mobile phone- and smartphone-based interventions may enhance active self-care among trauma survivors, extend the geographic reach of health-care providers, and facilitate the use of paraprofessionals and peer mental health support.⁵⁰

While these assessments are realistic, the focus on resilience, self-care and self-responsibilization is potentially problematic as a justification for digital health-care initiatives in fragile settings, because – as with prevention and early warning – their effectiveness hinges on the existence of digital literacy, trust, access and functionality, and on the effective mitigation of digital risk. A “safe space” is a questionable entity in the context of conflict: there is a high risk that one’s physical geolocation will be revealed and one’s personal data compromised. On the other hand, databases in themselves constitute potent targets for cyber attacks. The sensitive nature of health data means that the repercussions of negligent or inadvertent leaks and hacks can be serious not only for the digital body of the patient but also for her physical security. Furthermore, a digital user roadmap for services is only useful if the services are actually accessible to and meaningful for users.

Documentation

In the past, the cultural stigma attached to rape and the international community’s long-standing lack of attention to sexual violence in conflict have meant that little was known about this type of violence. Today, however, things are different. Here we identify two specific challenges to CRSV documentation, after first identifying some of the forms that CRSV data may take.

CRSV data can consist of surveys (victimization rates), medical data (such as patient medical records, medical certificates, and sexual assault medical forensic

49 Andrea L. Wirtz *et al.*, “Development of a Screening Tool to Identify Female Survivors of Gender-Based Violence in a Humanitarian Setting: Qualitative Evidence from Research among Refugees in Ethiopia”, *Conflict and Health*, Vol. 7, No. 1, 2013, available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC3695841/.

50 Josef Ruzek and Carolin M. Yeager, “Internet and Mobile Technologies: Addressing the Mental Health of Trauma Survivors in Less Resourced Communities”, *Global Mental Health*, Vol. 4, 2017; A. L. Wirtz *et al.*, above note 49.

examinations, commonly known as “rape kits”⁵¹), crime reports, perpetrator data, public (media) reports or proxy data (such as pregnancies resulting from rape). Such data can be used to reinterpret testimonies in order to identify formerly overlooked patterns of sexual violence, corroborate or confirm witness accounts and detect gender bias in documentation.⁵²

There are still many CRSV situations in which data may be non-existent or of poor quality due to collection problems, bias or “digital shadows” where access to digital devices and connectivity are limited;⁵³ effective data analysis may be hampered by low levels of data literacy in the practitioner community and so forth.⁵⁴ Yet, the problem is often no longer data scarcity. While UN Security Council Resolution 1325 of 2000 noted “the need to consolidate data on the impact of armed conflict on women and girls”, currently, CRSV actors—from field responders to international judges—are deluged with information about sexual violence, and need tools for data verification, analysis, and making responses operational and effective.

A different kind of challenge concerns the moral dilemma arising in the documentation of CRSV, from field responses to criminal prosecutions. This relates to the operational requirement for first-person testimony and the resulting practice, whereby survivors must conduct multiple interviews with multiple stakeholders, targeted towards multiple audiences. This practice, which may result in re-victimization, epitomizes one of the great failings of the sexual violence bureaucracy. The fundamental problem is the way survivor agency and ownership of the story comes up against institutional needs for credible evidence and believable narratives capable of generating empathy among politicians. With care, it might be possible to create a framework that would record and assess the veracity of victim testimonies from survivors, and ensure that they are the ones in control of the access codes—i.e., that there is one single gateway to the digital body for bureaucracies and service providers to scrutinize and engage with.⁵⁵

However, this solution also raises a number of issues, such as community acceptance, the standardization of process and quality, difficulties in guaranteeing the relevance of the statement to all stakeholder audiences, variations in end-user competence and digital acceptance, and problems related to unauthorized access,

51 Jaimie Morse, “Documenting Mass Rape: Medical Evidence Collection Techniques as Humanitarian Technology”, *Genocide Studies and Prevention: An International Journal*, Vol. 8, No. 3, 2014, p. 72.

52 Tony Roberts and Gauthier Marchais, “Assessing the Role of Social Media and Digital Technology in Violence Reporting”, *Contemporary Readings in Law and Social Justice*, Vol. 10, No. 2, 2018.

53 This lack of access to digital technologies is also known as the “digital divide”. For discussion on this term, see Lina Gurung, “The Digital Divide: An Inquiry from Feminist Perspectives”, *Dhaulagiri Journal of Sociology and Anthropology*, Vol. 12, 2018; Jennifer Radloff, “Digital Security as Feminist Practice”, *Feminist Africa*, No. 18, 2013.

54 Mark Latonero and Zachary Gold, Data, *Human Rights and Human Security*, Data & Society Research Institute, 2015.

55 Access codes are a series of letters and numbers that allow access. The idea, of course, is that legal regulations apply once consent to access has been given. The authors are grateful to the participants at the Expert Roundtable on “Using Tech Innovation to Combat Conflict-Related Sexual Violence”, held in Geneva on 18–19 February 2019 and hosted by Legal Action Worldwide and the Office of the UN High Commissioner for Human Rights, for this point.

destruction and manipulation.⁵⁶ Moreover, policies on the storage, sharing and destruction of such testimonies raise extremely difficult questions about ownership and control.⁵⁷ Digital technological approaches to documenting CRSV thus require participation and digital literacy to be made core components—but even when solutions are designed that focus on these objectives, old issues pertaining to the meaningful participation of victims/survivors will persist.

Accountability

Through digital devices, users produce a mass of data that can be used for establishing criminal accountability; this includes text messages, multimedia messages, metered data (numbers dialled, time and date of calls etc.), emails, internet browsing data, image, sound and audio files, and geolocation data.⁵⁸ For the prosecution of sexual violence, including CRSV, in a domestic or international court, new technology requires standardized and uniform digital forensic guidelines and methods (proper evidence handling, including preservation, storage and maintenance of the chain of custody) for the documentation, collection and preservation of both digital and physical evidence. Thus, digital forensic approaches to sexual violence require investigators, forensic scientists, medical staff and lawyers, among others, to have new types of expertise and training.⁵⁹

A different type of quandary relates to the institutional challenge of keeping in contact with witnesses, both to keep them apprised of developments and to get witnesses to testify when required. Technical solutions, but also political developments, make this increasingly feasible: in particular, digital identities are increasingly bound up with pushes for legal identity as an aim under Target 16.9 of the UN Sustainable Development Goals, whereby a legal identity is presumed to increase access to basic services, financial inclusion, social integration and regularization.⁶⁰ When wrapped into a digital format, legal identities make people instantly trackable. In the CRSV domain, this “trackability” presents some difficult issues: prosecutors’ offices and victims’ units obviously have an interest in finding ways to keep in touch with potential witnesses, and the difficulty of locating and communicating with survivors is a serious obstacle to adjudicating sexual violence crimes, but hard questions arise about the pros and cons

56 Marie-Helen Maras and Michelle D. Miranda, “Overlooking Forensic Evidence? A Review of the 2014 International Protocol on the Documentation and Investigation of Sexual Violence in Conflict”, *Global Security: Health, Science and Policy*, Vol. 2, No. 1, 2017.

57 For a good discussion of data protection in emergency contexts, see Ben Hayes, “Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and ‘Big Data’”, *International Review of the Red Cross*, Vol. 99, No. 904, 2017.

58 M.-H. Maras and M. D. Miranda, above note 56.

59 *Ibid.*

60 See UNHCR, *Global Virtual Summit on Digital Identity for Refugees, Concluding Workshop: Summary Conclusions and Recommendations*, August 2019, available at: www.unhcr.org/idecosystem/wp-content/uploads/sites/69/2019/12/Conclusions_and_Recommendations.pdf.

(including potential risks) of being a digitally accessible—and digitally identifiable—“stand by” victim of sexual violence.

Divergent perspectives on data: Tensions at the interface of humanitarian action, human rights practice and international justice

In recognition of the importance of data governance for the struggle against CRSV, the third part of our analytical framework interrogates how divergent perspectives on data may shape the pathways of CRSV data. In this section, we examine the implications of data extraction and use for humanitarianism, human rights and international criminal justice. These fields have been selected because they have a stronger legal tenor and are more closely interlinked than adjacent fields dealing with CRSV such as peacebuilding, development or transitional justice. A different scope—and a different set of analytical combinations—is of course possible.

Whereas humanitarianism sees misfortune and suffering, human rights sees injustice, discrimination and inequality. International criminal justice, in turn, sees atrocity, barbarism and impunity. We suggest that for the digital transformation of the struggle against CRSV, understanding the differences in how these three fields see survivor bodies—and the function and uses of digital bodies—is crucial. To sketch out how they relate to divergent perspectives on data, we consider some of the overlaps and tensions across these three different international response sectors⁶¹ and identify key structural differences between them in terms of their mission objectives, their time frames and their perceptions of individual and communal agency for those targeted for intervention. Our approach to the different sectors consists of so-called Weberian “ideal types”—simplifications used as analytical tools.⁶² This entails that we are not as concerned with hybridity and nuance within and among the sectors as we are with mapping out trends and tendencies. Neither is the critical and significant role of *domestic* actors considered. Instead, we aim to increase our understanding of how data collected by one particular actor for a particular purpose within a particular time frame passes on to other actors by being either borrowed or appropriated—and what the consequences of such transfers are. As such, we turn our attention to how background factors shape the different perspectives of humanitarianism, human rights and international criminal justice actors on “repurposing” data.

Animated by the call to “do something” about human suffering and global violence, the similar ethical and legal motivations of human rights, humanitarianism and international criminal justice have led to the widespread supposition that the

61 As noted previously, this section develops insights articulated in K. B. Sandvik, above note 6; see also Sara Kendall and Sarah Nouwen, *International Criminal Justice and Humanitarianism*, University of Cambridge Faculty of Law Research Paper 69, 2018.

62 See “Ideal Type”, *Encyclopaedia Britannica*, available at: www.britannica.com/topic/ideal-type.

spheres of these fields seamlessly overlap. In the cycle of intervention from early warning to accountability, the different sectors are seen as fulfilling complementary roles, each providing something needed by the others: humanitarians supply services, human rights actors look for truth, and international criminal justice produces legal accountability. Often, and this is the ideal, the cycle of intervention is imagined as running so smoothly that the sectors merge and blur into an uninterrupted course of action, as when human rights actors provide evidence for international criminal prosecutions, or when international criminal justice provides humanitarian relief through victim reparation. However, norms and good causes do not necessarily align just because we want them to.

In what follows, we disrupt this notion of unproblematic continuity from one sector to the next and consider some of the tensions between these sectors in relation to their use of data. It should be emphasized that these tensions concern issues of great practical significance. For example, the idea of human rights and international criminal justice actors using their beneficiary data is contentious for humanitarian actors, as it may threaten their principles of neutrality and impartiality and accordingly cause harm by limiting their humanitarian access. For these reasons, some humanitarian organizations have policies of non-cooperation with the International Criminal Court.⁶³ In other words, despite their shared ethics of addressing human suffering, the sectors operate with divergent views of who they can legitimately borrow, extract or receive data from. The differences between the humanitarian, human rights and international criminal justice sectors thus lead to different perspectives on how to harvest, manage, use and share data. In what follows, we show how these tensions are embedded in the objectives of the different sectors, and in their relationship and approach to time and agency.

Objectives

The different views and approaches to data are closely related to the different agendas of each sector. The aim of humanitarianism is to address needs and save lives, which entails that it—in theory—has little concern for the connection between justice and peace. Human rights aims to provide accountability, transparency and justice, whereas international criminal justice is interested in establishing and adjudicating individual criminal responsibility and legal punishment; it sees criminal justice as a precondition for peace. While the “politicization” of emergencies—including situations of mass violence—is a problem for humanitarianism because it may interfere with the response to humanitarian needs, human rights actors, from their perspective, may consider

63 Fabrice Weissman, “Humanitarian Aid and the International Criminal Court: Grounds for Divorce”, Centre de Réflexion sur l’Action et les Savoirs Humanitaires, Fondation Médecins Sans Frontières, 2009, available at: www.msf-crash.org/en/publications/rights-and-justice/humanitarian-aid-and-international-criminal-court-grounds-divorce.

trade-offs in the interests of producing accurate, credible data and securing formal rights protection. These differences matter in terms of what data can be used for. They also matter for secondary objectives: while persuasion, public condemnation and prosecution are complementary modes of action in response to CRSV, they also involve significant tensions regarding the proper handling of data. This might include contestations over how data is collected and the “proper” norms of its collection; data ownership and questions with respect to the interests driving the consolidation of databases; and also issues of consent (what is good enough, how long does it last and for what uses may it be extended?).

While their mandates differ, as does their support for criminal prosecutions, most humanitarian organizations support prosecution as a response to breaches of international criminal and humanitarian law, including CRSV.⁶⁴ However, humanitarian organizations may be reluctant to participate in judicial processes because doing so may jeopardize humanitarian access to vulnerable populations.⁶⁵ For this reason, humanitarian actors may choose not to actively participate in international criminal procedures, as the “purpose of humanitarian action is, above all else, to save lives, not to establish criminal responsibility”.⁶⁶ Human rights organizations have shown much more willingness to contribute to international criminal prosecutions.⁶⁷ Human rights NGOs are at the forefront of the fight against impunity for CRSV, as the criminal justice system offers a tool to enforce human rights.⁶⁸ Reports by human rights organizations have therefore also been submitted as evidence before international criminal courts and tribunals. This practice has attracted significant criticism,⁶⁹ precisely because of the different mandates of human rights and international criminal justice actors and what this means for their respective approaches to data. These differences also determine how and to what extent the digital bodies of CRSV victims/survivors are drafted into the accomplishment of institutional objectives.

Temporalities

There are also important temporal differences between the three sectors. To return to the cycle of intervention, humanitarian actors are often first to the scene, and may possess first-hand information on sexual violence, survivors and perpetrators. They may also have knowledge of the nature and scale of the violence, including whether

64 Anne-Marie La Rosa, “Humanitarian Organizations and International Criminal Tribunals, or Trying to Square the Circle”, *International Review of the Red Cross*, Vol. 88, No. 861, 2006.

65 *Ibid.*

66 *Ibid.*

67 Kjersti Lohne, *Advocates of Humanity: Human Rights NGOs in International Criminal Justice*, Oxford University Press, Oxford, 2019. See also Kjersti Lohne, “Penal Humanitarianism beyond the Nation State: An Analysis of International Criminal Justice”, *Theoretical Criminology*, Vol. 24, No. 2, 2020.

68 Karen Engle, Zinaida Miller and Denys Mathias Davis, *Anti-Impunity and the Human Rights Agenda*, Cambridge University Press, Cambridge, 2016.

69 In the International Criminal Court’s very first prosecution, the case against the Congolese militia leader Thomas Lubanga, the use of so-called secondary evidence was heavily criticized. See Elena Baylis, “Outsourcing Investigations”, *UCLA Journal of International Law and Foreign Affairs*, Vol. 14, No. 1, 2009.

what has been done meets the criteria for crimes against humanity, war crimes or genocide, which may make it eligible for international prosecution. Similarly, human rights organizations may call attention to and document instances of CRSV in close to real time. International criminal justice actors, on the other hand, are rarely first to the scene. Indeed, they are dependent on data from other actors – State and non-State – to successfully investigate and prosecute CRSV. These different temporal positions in the cycle of intervention matter for how and for what purpose data is collected, managed and passed on. As such, timelines not only create different types of digital bodies, but also shape the kind of work that digital bodies are put to.

As such, the three sectors work with and imagine different time horizons. Humanitarianism operates in the ongoing state of emergency, addressing the needs and suffering of the present to bring relief in the urgent future.⁷⁰ For humanitarians, the time horizon is short; in theory at least, what matters most is today and tomorrow. This makes data management part and parcel of the day-to-day governance of vulnerable populations. While it is possible to trace and establish responsibility for harms committed, human rights and international criminal justice operate on a much longer time frame. They seek to address individual and systemic injustices of the past in order to establish accountability, provide redress and prevent future violations of human rights and international law. The long-term goal of human rights and international criminal justice is the institution of a universal moral and judicial community. This being so, these temporal differences also reflect a difference in audience and, critically, in how these sectors view the agency of those they address.

Agency

A final issue thus concerns agency. While all three fields are cosmopolitan in orientation, meaning that they have a “philosophical, ethical, and scientific world view which aims to transcend national boundaries and a nationalist, state-centered outlook on society and justice”,⁷¹ their actions are strongly oriented towards States and donors, and their institutions and practices reflect donor priorities.⁷² How will this change when tech actors enter the scene? For example, “[a]s social media increases in importance, so do the social media companies themselves. Facebook, YouTube, Twitter, etc. are all corporations, and they host the videos, photos, and reports that are posted to social media on privately-owned data

70 Although humanitarian actors have been present in some locations for several decades and are increasingly present in protracted conflicts, a state of emergency animates their intervention; see Didier Fassin and Mariella Pandolfi, *Contemporary States of Emergency: The Politics of Military and Humanitarian Interventions*, Zone Books, New York, 2010.

71 Cecilia M. Baillet and Katja Franko Aas (eds), *Cosmopolitan Justice and Its Discontents*, Routledge, London, 2011, p. 1.

72 S. Kendall and S. Nouwen, above note 61.

servers.”⁷³ Moreover, while all three sectors push for professionalization that “favours ‘technical’ and generalizable knowledge of local communities”,⁷⁴ these developments may also increase the distance between staff and victims/survivors. Questions must therefore be asked about how digital technologies factor into recurrent criticisms of justice that is distant and remote, rather than place-based, and the extent to which technological solutions facilitate or hinder survivors’ participation. This also affects how we think about the freedom to engage. Scholars have increasingly begun to ask critical questions about the freedom not to engage with the data market or not to be represented on commercial databases.⁷⁵ In our context, this entails asking how much visibility survivors of CRSV owe the state, the international community or the aid sector, and whether their digital bodies should automatically be enlisted in the fight against impunity for sexual violence when technology facilitates the collection of evidence.

Conclusion

This article has offered a three-part analytical framework for investigating the possibilities and pitfalls of the ongoing digital transformation of the fight against CRSV. In particular, we have proposed the use of “digital bodies” as an analytical concept for facilitating cross-sectoral exchanges on power and responsibility in data governance.

Despite good intentions, technology does not always work as planned or intended. Inadequate problem definition may entail that technological solutions fail to respond to the real-life issues that they are set up to deal with. A widespread reason for flawed problem definition remains the fact that affected populations are often not present in innovation processes—they are neither properly consulted nor invited to participate.⁷⁶ We therefore suggest that the international community must pay further attention to the serious ethical and legal issues emerging from technological innovations within the aid sector: technology has the potential to produce new digital harms, whether these occur through (in)visibilizing the suffering of particular groups or individuals, creating undesirable consequences, or introducing new risks.

There is also a need to distinguish clearly between what technology does and does not see when addressing CRSV. We noted above that the dual focus on technology and sexual violence potentially generates a powerful moral economy, but that it is important to consider the extent to which one issue—sexual

73 Emma Irving and Jolana Makraiová, “Capture, Tweet, Repeat: Social Media and Power in International Criminal Justice”, in Morten Bergsmo, Mark Klamberg, Kjersti Lohne and Christopher B. Mahony (eds), *Power in International Criminal Justice*, Torkel Opsahl Academic EPublisher, Brussels, 2020.

74 S. Kendall and S. Nouwen, above note 61.

75 Linnet Taylor, “What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally”, *Big Data & Society*, Vol. 4, No. 2, 2017.

76 Mirca Madianou, Liezel Longboan and Jonathan Corpus Ong, “Finding a Voice through Humanitarian Technologies? Communication Technologies and Participation in Disaster Recovery”, *International Journal of Communication*, Vol. 9, No. 1, 2015.

violence – can crowd out other issues and framings of CRSV and related insecurities. At the same time, increased reliance on digital evidence may alter the types of crimes and victim subjectivities that get attention (and documentation), and may unintentionally contribute to the (re)silencing of sexual violence and CRSV in the face of more explicit criminal imagery – killings, for example.⁷⁷ It is also worth considering the extent to which digital technologies – and social media especially – exacerbate issues related to stigma, shame, and re-traumatization and secondary victimization. In short, digital technologies do not solve political and ethical problems.

Finally, we suggest that a deeply problematic aspect of the digital turn is the trend towards extraction of data in exchange for aid, protection and justice. From an emancipatory – and a feminist – perspective, this necessitates the inclusion of participation and investment in digital literacy as key aspects of a technologized approach to the struggle against CRSV. Digital literacy must be mainstreamed to include all actors, from survivors and field practitioners to stakeholders in humanitarian, human rights and international criminal justice responses. To that end, impact assessments, training and capacity-building around cultures of responsible digitalization are needed. Digital literacy can only be acquired when survivors and community members are empowered to build, trust and act on this capacity, and when donors and policy-makers are committed to investing time and resources. Participation is thus key to successful technologized interventions, and stakeholders should bear this in mind when deciding on their actions and interventions.

77 E. Irving and J. Makraiová, above note 73.