"Is technology an opportunity or a threat for human rights lawyers? Does it increase or reduce risks for lawyers in carrying out their duties and in what circumstances might technology be used to mitigate such risks?"

This essay explores the parallel potential and problems for human rights lawyers in using technology to carry out their duties. It will distinguish between 'support technologies' and 'information communication technologies (ICT)', and further outline the opportunities for use and abuse of each. It will argue that technology is an opportunity for human rights lawyers to increase victim participation and improve efficiency, but one that simultaneously incurs evidentiary, ethical and security concerns in respect of the storing and sharing of big data.

Support Technologies

Common challenges faced by human rights lawyers include: cases that can last for years; complications from working in multiple jurisdictions and in different languages; and withstanding pressure and/or surveillance from adversaries, whether they be states, corporations or individuals. Three forms of technology are being touted for their ability to support lawyers in executing their duties most effectively. They are: (1) Case management tools (2) E-discovery tools, and (3) Investigation and case building tools.

Case management technology better enables a lawyer to manage the day-to-day flow of case information, such as client details, the exchange of documents and important dates. E-discovery tools then permit the digitising of potential evidence for review. They also make these documents searchable by metadata i.e. names and places, which streamlines the process of understanding what is relevant. Investigation and case-building tools then allow a lawyer to analyse relevant information by producing visual overviews such as timelines or network diagrams of the particular persons of interest. CaseMap - an example of such technology – has been used to great effect by the International Criminal Court and the Extraordinary Chambers in the Courts of Cambodia. Technology-assisted review by way of predictive coding has also been mandated in certain cases following *Brown* v *BCA Trading*.[1]

These technologies boast huge potential for making the work of human rights lawyers more efficient and effective. However, they also serve to exemplify a paradox at the heart of this essay's calculation: by using technology to fight for a client's human rights, lawyers also run the risk of violating a client's right to privacy. The digitising of sensitive information through document storage or online communication makes otherwise privileged material potentially subject to surveillance. The erosion of freedom of expression in the digital space due to fear of surveillance, and the ways in which this trend

[1] [2016] EWHC 1464 (Ch).

is particularly detrimental to the work of a lawyer, was highlighted in a June 2015 report by UN Special Rapporteur David Kaye.[2] However, safeguards for lawyers' online activity have not been forthcoming.

A recent landmark judgment of the European Court of Human Rights[3] found that the UK's historical bulk interception regime violated Article 8 of the European Convention on Human Rights (ECHR), the right to privacy, and Article 10, the right to freedom of expression. Although it is a significant step forward in protecting online privacy, it nonetheless permits national governments a wide margin of appreciation in deciding whether to engage in mass interception – the court approves of interference that is "necessary in a democratic society", a test that is variable by nature. Encryption could be a means for lawyers to avoid technology becoming a double-edged sword, although a burdensome one. Encryption protects the integrity of content by converting data or messages into a form that is readable solely by the intended recipient. While this could help to protect client-lawyer confidentiality, its potential use sits uneasily with the currently poor level of technology literacy within the legal field.

Information Communication Technology (ICT)

ICT is being used for monitoring and documenting human rights violations. WITNESS and eyeWitness are two technologies used by citizens to capture footage of violations, which is then analysed and verified. Herein lies a particular challenge for human rights lawyers: while these technological developments have fostered awareness through evidence gathering, lawyers must ensure evidential integrity in order for this technology to generate accountability. If user-generated material is to be considered evidence, it must first be determined reliable. There are three significant hurdles to overcome in this regard: (1) the consent of the people featured in the material, (2) the completeness of the evidence and (3) the possibility of doctored data.

Firstly, assumptions should not be made as to whether the people represented in the material are aware that it is being stored and analysed for human rights purposes. This difficulty could, in some instances, be overcome using the likes of YouTube's face blurring tool which facilitates both the use of material and the protection of anonymity. Secondly, video evidence does not displace the need for substantiation by way of eyewitness or victim testimony, nor does it remove the importance of thorough investigations of crime scenes. User-generated data is particularly useful in identifying that a violation occurred, but is often insufficient to link a perpetrator to said crime. For example, video evidence of an atrocity that features particular soldiers with identifiable uniforms is a useful clue for investigating a crime. If an investigation was subsequently launched in which spent ammunition that is traceable to that particular military unit was found, it could be used to help establish a more definitive link between the soldiers

[2] OHCHR, 'Report on encryption, anonymity, and the human rights framework', 2015, https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx.
[3] Big Brother Watch and Others v. the United Kingdom (nos. 58170/13, 62322/14 and 24960/15)

featured and the atrocity. The video evidence thus serves to shape our understanding of the context in which a violation occurred, which as noted by Stanley Cohen, helps to offset potential use of a tactic he calls 'literal denial' i.e. it requires the accused to provide an alternative explanation for their activities or to show that their actions are justified.[4]

It is argued that the balance to be used by human rights lawyers is this: user-generated data should be used to corroborate, rather than replace, more traditional forms of evidence. A secondary reason for this is the risk of establishing a culture of 'seeing is believing' within the law. If juries become sensitised to, and reliant upon, seeing audio-visual evidence of the alleged violation, it could result in them being less likely to believe accounts that are not represented in this manner. Moreover, given the likelihood that user-generated data will be of poor quality, it may lead to doubts regarding the authenticity of the material. This possibility feeds a pre-existing problem for human rights lawyers using technology to carry out their duties: the potential for doctored data.

Doctored content does not require the staging of material but can also take the form of manipulating the context portrayed. For example, videos or images from one context can be scraped and repackaged as representing another; this is done by manipulating the metadata of the material such as the time and date. This has occurred on YouTube many times when videos are reposted using different captions – the same video has been referred to as depicting Colombian Special Forces assailing a farmer, Venezuelan Armed Forces assaulting a student, and Mexican Police aggravating an activist.[5] The ensuing responsibilities for lawyers to ethically triangulate data and to assess its biases and defensibility led Eva Galperin to state that "technology overstates the problems it can solve."[6]

Mitigating the Risks of Technology

Resources exist to help lawyers mitigate the risks of technology that have been outlined so far in this essay. Berkley Law School has launched a 'Technology and Human Rights Program', which focuses on data accountability issues and forensic methodologies. This is essential for transforming technology into an investigative technique fit for human rights law. The project currently supports the International Criminal Court to strengthen its capacity in security, software, analytics and open source intelligence; this is particularly important given that procedural rules at international courts and tribunals are relatively silent on what factors are necessary for authenticating new forms of electronic evidence. A

[4] S. Cohen, *States of Denial: Knowing about Atrocities and Suffering* (Cambridge: Polity Press, 2001), p. 7.
[5] M. Bair and V. Maglio, "Video Exposes Police Abuse in Venezuela (Or Is It Mexico? Or Colombia?)," *WITNESS Blog*, February 25, 2014,http://blog.witness.org/2014/02/video-exposes-police-abuse-venezuela-mexico-colombia/.
[6] Interview with Eva Galperin, August 20, 2013.

report on human rights electronic evidence outlines that courts still apply standard evidentiary rules and thus have regard for authenticity, protection of privacy, chain of possession and reliability.[7]

The United Nations is also partnering to increase its technological capacities vis-à-vis human rights. Together with Microsoft, they launched a dashboard called 'Rights View', which can aggregate artificial intelligence and big data analytics in order to verify reported human rights abuses. This is done by cross-checking allegations against other data sets and by searching for additional clues. This form of technological advancement was central to the building of Amnesty's case to implicate Myanmar military officials in atrocities committed against the Rohingya.[8] Throughout the campaign of violence that included unlawful killings, torture, rape and village burnings, Amnesty employed satellite imagery to detect which villages were being targeted – this helped to demonstrate the deliberate nature of the attacks. It also examined metadata in hundreds of photographs and videos, which was then matched with features in a verified source, satellite imagery, in order to authenticate the material. This authenticated material served to corroborate the first-hand testimony of survivors and witnesses in both Bangladesh and Myanmar. The combination of these evidentiary sources allowed Amnesty to detail how the military carried out large-scale massacres in the villages of Chut Pyin, Min Gyi and Maung Nu, as well as to identify specific military units that were responsible.

Conclusion

The Nobel Peace Prize laureate, Christian Lous Lange, highlighted the dual potential and problems of technology when he said: "technology is a useful servant but a dangerous master."[9] Opportunities abound for human rights lawyers to work more efficiently and effectively by using technology to document and report human rights violations, as well as to map trends and patterns using big data. However, this essay has also outlined the evidentiary, ethical and security concerns that frame the push for data literacy amongst lawyers. We must, therefore, remain alive to the fact that while technology has expanded our means of exercising human rights, it has also transformed our means of violating them.

---

[7] Center for Research Libraries, 'Human Rights Electronic Evidence Study', February 2012, http://www.crl.edu/sites/default/files/d6/attachments/pages/HREES_Final_Report_Public.pdf.

[8] Amnesty International, 'We Will Destroy Everything: Military Responsibility for Crimes Against Humanity in Rahkine State, Myanmar', 2018, https://www.amnesty.org/download/Documents/ASA1686302018ENGLISH.PDF.

[9] 'Christian Lange Nobel Lecture' (*The Nobel Prize*, 13 December 1921) <https://www.nobelprize.org/prizes/peace/1921/lange/lecture/> accessed 15 November 2018