Big Data and Technology

Big Data and Technology: A Discussion

Elena Abrusci, Antonio Coco, Talita de Souza Dias, Audrey Guinchard and Sabrina Rau
[DOI: 10.5526/xgeg-xs42_033]

Several of the authors in this section took some time to discuss some of the common themes that arose in their papers and the synergies between them.

It was recognised that states have an obligation to counter the spread of mis-information regarding Covid-19. This stems from their obligations to protect, respect and fulfil the right to life and right to health. States' due diligence obligations are important in this regard, particularly when the evidence is insufficient to find states responsible for the outright breach of rights; they would nevertheless have obligations for which they could be found responsible to exercise due diligence by taking appropriate steps to forestall the abuses.

Whether states will be responsible when individuals follow "fake news" advice, for example will depend on who creates and disseminates the fake news. There is a clear connection to state responsibility when state leaders are directly responsible for creating and spreading the harmful fake news themselves. When non-state actors spread the news, the state can be responsible in a secondary sense for failing to exercise due diligence to protect against the online spread of fake news which is detrimental to life or health, though this may not necessarily extend to liability for the actions taken by private individuals who act in furtherance of the fake news. The boundaries between the prevention of mis-information and censorship will depend on the facts in a particular case. The prevention of mis-information about health during a pandemic is perhaps a clear issue, whereas states' role in preventing the spread of other types of mis-information outside of an emergency context may be closer to censorship; the boundaries are not always clear. Many of the digital platforms are privately owned and the UN Guiding Principles on Business and Human Rights have a normative framework which addresses such issues, though businesses' engagement with it is voluntary. Nevertheless, it was recognised that few states have been willing to go so far as to interrupt tech companies' business model related to paid advertisements – the usual source of fake news. Instead, efforts have so far focused, mainly, on calling for greater transparency for political ads.

Discussants recognised the complexities of the due diligence concept which had slightly different meanings under the laws of state responsibility and corporate responsibility, and depending the types of harms involved. Also, the timeframe as to when due diligence [illegible] under human rights law, the obligations are activated at an early stage given the focus on preventing violations. This is not necessarily the case with other subsets of public international law. Clearly, the timing of obligations is important for the prevention of online harms, given the fast pace in which information is disseminated.

With respect to the "do no harm" principle, discussants considered whether it was a sufficient basis to foster greater compliance by states and tech companies with their obligations. For states, due diligence refers to exercising best efforts. The content of what "best efforts" might entail in a given context is less clear. For businesses, there is arguably a clearer meaning of what due diligence means, especially in respect to the procedural

steps businesses should be taking to identify and respond effectively to risks, as set out in the UN Guiding Principles. Greater clarity on the content of due diligence may be difficult to achieve, because it is so context specific. Also, particularly from the Business and Human Rights perspective, there is a constant need to balance different rights (expression, privacy etc) and a more content-led definition may impede the necessary balancing exercises. Also raised was the need for standards to accurately set out the need for continual due diligence, to better account for technological advancements after products are unleashed, and/or for new circumstances giving rise to new or heightened risks. The ongoing research of Coco and de Souza Dias is currently assessing the content of due diligence rules within the different sub-disciplines of public international law, to look for commonalities, and potentially evidence of any general principles of international law. Further consideration of how the principles are applied domestically in different tort law contexts may equally be a useful area for further research.

Discussants also considered the important discipline of data protection, an area canvassed by Guinchard in her paper and broader research. The interpretation of “personal data” within data protection legislation is broad, which provides another avenue for the protection of privacy and the policing of online content. Data protection frameworks incorporate the balancing of rights and set out detailed procedural rules, however enforcement has been weak, so tech companies have often escaped scrutiny. Also, the ways in which the laws are enforced country to country differs significantly. There is a lack of transparency from companies related to disclosure of what data they own and how they use it, but equally, states and public institutions lack political will to press tech companies too hard. This also becomes a problem of due diligence, whether states are taking adequate steps to meet their due diligence obligations in respect of tech companies.

When states collaborate directly with tech companies, the problems tend to be magnified. Neither party has satisfactory procedures in place, and thus the combination simply accentuates the unsatisfactory procedures, and the state becomes even less well placed to enforce regulations. With respect to data misuse during Covid-19, there is relative transparency about the data to be used by the UK’s planned tracing App. What is less clear is the data store, and it is also unclear what data the government will be seeking and using from private companies.