CASE STUDY: GENERAL DATA PROTECTION REGULATION – A GLOBAL STANDARD?

Steve Desilets

MSDS 485: Data Governance, Ethics, and Law

October 15, 2023

1. Introduction

In an article in *Surveillance and Society*, Dr. Payal Arora explores the intricacies of how regulators that sincerely want to protect the data privacy of digital consumers may have accidental negative consequences unless policymakers carefully tailor and enforce such legislation in a way that intentionally empowers marginalized individuals in each society (Arora 2019). In this paper, we delve into the specifics of her article, "General Data Protection Regulation – A Global Standard" and examine the data, relevance to data governance, relevant legislation, and data governance solutions that are highlighted in this piece.

2. The Data

Since Dr. Arora focuses on legislation that would apply to nearly any digital data shared by consumers online, the definition of data in this article is quite broad. As the author explains, data can refer to something as seemingly benign as individuals sharing their recent purchases with social media followers to something as private and personal as biometric data, such as iris scans. Similarly, the analyses conducted using these datasets vary greatly in their scope and level of sophistication. The types of data analyses that Dr. Arora explains would be affected by her policymaking suggestions range in sophistication from gang members casually reading individuals' locations on social media posts to sophisticated real-time surveillance systems that alert the Saudi government about migrant workers' locations. In essence, the data and analyses on which Dr. Arora focuses in this article is all online data with particular emphasis on online data collected from marginalized communities.

3. Relevance To Data Governance

Though there are four pillars of data governance (data stewardship, data quality, master data management, and data governance use cases), this article is primarily relevant to the pillar of data stewardship, which focuses on implementing policies related to data management, legal compliance, and ethics. Data stewardship is a particularly prominent theme in this piece because the focus of the article resides at the intersection of ethics and law. Specifically, the article advocates for the law and its enforcement to reflect the ethical needs of local, marginalized populations by challenging traditional data privacy regulators to rise to the occasion of addressing five calls-to-action. These five measures would address mitigating activists' longstanding distrust of the law, channeling efforts into local (rather than international) digital regulations, advancing communities' collective rights, meeting the needs of individuals who need publicity more than they need privacy, and re-framing activism as everyday creative insurgencies. While the primary focus of this article is on ethics and legislation, if societies adopted the author's policy prescriptions, then the impacts of such a move would also trickle down to influence organizations' data management operations as well.

4. Relevant Legislation

Prescriptions for how to improve data governance legislation lie at the heart of Dr. Arora's article. For example, the author explains that policymakers should carefully craft and communicate legislation related to digital protections– especially in repressive societies where individuals (especially activists) have been subjected to generations of surveillance. Lawmakers must intentionally explain how well-intentioned legislation, like India's massive biometric identity project aimed at streamlining citizens' access to social services differ from historical, repressive legislation like the Sedition Law Act of 1870, which British rulers enacted to silence Indian activists via similar biometric surveillance techniques. The article also cites many examples of how the design and enforcement of digital privacy legislation should be community-focused and explains how even well-intentioned transnational legislation like the EU General Data Protection Regulation (GDPR) would fail to protect a resident in a Brazilion favela from being robbed by someone in their local community who monitors their location on social media.

5. Data Governance Solution

The key takeaway from this article is that since the needs of the general public (and more specifically, the needs of marginalized communities) vary from place to place, legislation designed to protect communities should also meet the needs of those communities. The author cites many such community-specific data governance needs, such as the Uighurs needing support for digital collective action and protection from group discrimination, women needing the freedom to access public resources on the internet without peer interference, and dissenting voices from activists needing to be heard rather than silenced by governments, companies, and regulators. In summary, governments and organizations must take local cultures, traditions, and needs into account when enforcing global data governance laws and policies. These entities must intentionally operationalize (and police) data governance in a way that advances social justice so that laws and policies designed to protect individuals digitally don't accidentally cause further harm instead.

References

Arora, Payal. 2019. “General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South.” *Surveillance & Society* 17 (5): 717–25. https://doi.org/10.24908/ss.v17i5.13307

Eye on Tech. 2020. “What is Data Governance? How Does it Impact Businesses?” YouTube, 2:16. February 14, 2020. https://www.youtube.com/watch?v=BqdPuwvwPk4