



# MY DATA RIGHTS

## Feminist Reading of the Right to Privacy and Data Protection in the age of AI

By Chenai Chair

# Executive Summary

The triple threat of high inequality, poverty and unemployment, remnants of colonisation and apartheid adversely affects women, gender diverse people and sexual minorities more at various intersections including race and class. The crisis of gender-based violence disproportionately affects women, girls, and non-gender conforming individuals such as lesbian, gay, bisexual, transgender and/or intersex people. The existent injustices that marginalised groups and sexual minorities face shape how they experience technology, policy, and regulation – either to achieve social justice or increase current inequalities and harms.

In the era of AI based innovations such as automated decision making and algorithms this context is important to understand how we can safeguard against harms and injustices while using these technologies to dismantle barriers of oppression. The development, implementation and governance of AI based innovations, especially around data that is fed into them, raises important questions on their impact on society and digital rights.

## **This research seeks to respond to the following questions:**

- 1) What would a gender-responsive data protection and privacy law entail to ensure gender safeguards against AI gendered harms?
- 2) How can civil society play a role in ensuring a gender transformative law and practice with a focus on the right to privacy and data protection?

The feminist conceptual lens draws from data feminism, intersectionality, data justice and feminist principles of the internet. The conceptual lens allows one to ask questions of who is being represented and by whom; whose interests are being centered; why this discussion is important and how it is taking place, which allows for criticism of power and how data itself can be used to ensure justice in society.

The methodological approach for this paper includes qualitative interviews to understand the current AI ecosystem and related privacy and data protection laws in South Africa. A targeted quantitative survey with open ended questions was shared with selected activists that work on gender and sexual justice issues to gauge perceptions of concerns with privacy and data protection. Recommendations on how civil society may intervene were drawn from there. The necessary ethical protocols were followed based on feminist internet ethical research practices.

## **This paper identifies the following key takeaways:**

### **AI Discourse in South Africa**

AI innovative solutions are on the rise in South Africa largely being driven by the private sector's need for a competitive edge in markets and the public sector's need for efficient developmental solutions. Policy conversations on governing AI have begun in the country with a focus on ensuring economic gains through the creation of employment opportunities by upskilling citizens; being innovative enough to attract global business as well as legal and regulatory compliance for global trade. The Presidentially appointed Fourth Industrial Revolution Commission has recommended the establishment of an Artificial intelligence institution. However, concerns have been raised that there is a risk of perpetuating digital disparities and inequality in the discourse around AI.

### **Uneasy Access - Gendered concerns of AI**

The right to privacy from a gender perspective is particularly important as access to digital platforms may be problematic for women and gender diverse people with continuation of existing patriarchal dynamics online from offline realities. Issues emerging from a gender perspective include the lack of agency and control over data, problematising consent in contexts of unequal power dynamic, loss of privacy, discrimination, and bias at the intersection of race, class, and gender.



## Perceived concerns of AI harms

The research conducted finds that there is in general a lack of documentation on harms in the South African context. For the purposes of this paper, five AI scenarios were therefore given to survey participants for them to reflect on how these harms would play out in the South African context and in relation to their areas of work. Key contextual issues that were recurring references were race, economic status, homophobia, and gender-based violence. The issues around bias, discrimination and increased surveillance were raised as likely to be of concern.

## Responsiveness of current Protection of Personal Information Act to AI and gender issues

The country's Protection of Personal Information Act (2013) is the focus of assessment as it is an existing regulatory framework that has relevance to both the current governance of data and AI, as well as the conceptualisation and interpretation of new policies in this space. As the law was set up close to two decades ago there are significant gaps with AI specific provisions although there is a safeguard for automated decision making. The analysis found a need for the current law to be contextually responsive, address the issue of gender exclusionary language (he/she used in the text) and the lack of nuance of gender and sexuality harms embedded into the law. There were examples of civil society making use of the law to challenge surveillance issues however a gendered nuance is missing.

To be gender responsive means to design and implement policies that consider gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development. The following recommendations are put forward on how this can be done with diverse stakeholders.

## The areas of recommendations stemming from this paper cover four important areas.

1) Policy and regulation:

Policy and regulation would require context-based implementation and assessment of current and future privacy and data protection laws with regards to Artificial Intelligence innovations. This would be complemented by collaboration between Civil Society, the legal community, and other relevant stakeholders.

2) Research and documentation:

Research and documentation are necessary to fill the knowledge gap in understanding the context-based impact of AI based innovations. Case studies documenting the impact of AI on marginalised groups would highlight the necessary responsive means to safeguarding against harms and injustices. Research may also be used to support development of governance models and develop AI registrars to document the proliferation of AI, where it is used and the impact it has. Resourcing these initiatives to ensure their public and open resources is important.

3) Public awareness:

Public awareness requires collaborative, relatable, and innovative campaigns to raise understanding of the opportunities and challenges of AI with regards to privacy and data protection. Public awareness would focus on campaigns for diverse marginalised groups, creation of collaborative spaces that are safe for gender and sexual minorities to learn and raise their concerns and resourcing from different stakeholders to ensure the necessary support needed for public participation

4) Responsibility of technical community:

The technical community carries the responsibility of carrying out public engagement and sharing information on how their systems work to ensure accountability and trust of AI based innovations. Civil society can be drawn into ethical guideline development that is cognisant of experiences of injustice for marginalised groups. In design and implementation of AI based solutions – digital literacy, privacy by design and context responsiveness should form underlying guiding principles in designing solutions that would not lead to further social injustices.

