


 HEINRICH
BÖLL
STIFTUNG
BRUSSELS

 HEINRICH
BÖLL
STIFTUNG
WASHINGTON,
DC

E-PAPER

Shaping the Future of Multilateralism

Does data protection
safeguard against
gender-based risks
in Southern Africa?

BY CHENAI CHAIR

Published by Heinrich-Böll-Stiftung, July 2021

About the author

Chenai Chair *is the Special Advisor on Africa Mradi Innovation at Mozilla Foundation.*

She is an expert on the intersection of digital technology and gender. She has built her expertise with extensive experience in work that is focused on understanding the impact of technology in society through research and public policy assessment. Her work draws on principles of feminism in assessing digital technology. She has developed projects focused on privacy, data protection and AI as Mozilla 2019/2020 fellow – available on mydatarights.africa. She also led the research on Women’s Rights Online as the Web Foundation’s gender and digital rights research manager. She has worked on issues of access within the digital divide as a Researcher at Research ICT Africa (RIA). While at RIA, she developed communication strategies to increase public engagement on research as a Communications Manager. She also works as a consultant on research projects focused on digital rights including assessing the state of digital identity in Zimbabwe and developed recommendations for digital rights literacy in Southern Africa. She is currently an Internet Governance Forum Multistakeholder Advisory Group Member and a steering committee member for The Center for International Governance Innovation’s work on assessing online Gender Based Violence. Chenai holds a Masters in Social Science degree focused on Global Studies from the University of Cape Town.

Contents

Does data protection safeguard against gender-based risks in Southern Africa?	4
Multilateral policy development on data protection: the EU and Africa	5
Feminist framework	6
Protecting data related to gender and sexuality	7
Recommendations for safeguarding sexuality and gender data	11
Conclusion	13
References	18

Does data protection safeguard against gender-based risks in Southern Africa?

The increasing data-driven nature of societies raises concerns about how to prevent data misuse and abuse that may harm individuals and communities, particularly marginalized groups. A feminist critique of the model law on data protection of the Southern African Development Community and the EU's GDPR, however highlights the dangerous gaps that place women and gender-diverse people at risk.

Multilateral systems are often based on the assumption that peer-to-peer interactions occur at equal degrees of power and with equal understanding of the mechanisms and bureaucracies involved. But while multilateral frameworks hugely influenced the independence and development – or underdevelopment – of African countries, leaders of the region [question](#) the extent of their power and the meaningfulness of their involvement in these mechanisms, considering the imbalance in relation to stronger states and institutions.

In the development and implementation of digital policy and regulation, the EU and other established multilateral organizations are often ahead of Africa, based on historical context, capacity, and financial strength. While Africa is still focusing on closing the digital divide and increasing connectivity, the Global North is looking at advanced issues related to digital rights, data, and data-driven technologies, to ensure the protection of human rights and social, political, and economic justice.

Despite these differences in their stages of development, all countries involved have a need to coordinate on emerging issues. Such alignment eases regional trade, creates a conducive environment for multilateral economic and social support, and ensures cross-border security, especially in relation to data privacy and data protection.

The fact that societies are becoming more and more data-driven raises concerns about how to ensure fundamental human rights by safeguarding against data misuse and abuse that may harm individuals and communities, particularly in marginalized groups. Users may not even be aware of [the large amounts](#) of data that are being collected, stored, used, and disseminated by private and public entities, much less be conscious of the potential impact. Data is often processed in contexts of power imbalances, with a few big tech companies holding enormous amounts of data across the globe. Data protection theoretically provides a means to safeguard personal data when processing it may harm or pose risks to, for example, health, finances, or personal safety.

A feminist critique of whether and how well data protection addresses issues related to gender and sexuality can provide essential perspective, especially when multilateral systems are supporting national or multinational policy development. A feminist framework asks questions such as:

- What are the concerns related to gender and sexuality?
- Do the current data-protection frameworks address these issues?
- What is needed to ensure gender is fully taken into account within data protection?

One illustration of this point can be found in examining how the processing of gender- and sex-related data is addressed in the European Union's 2016 General Data Protection Regulation (GDPR) and a 2013 model law on data protection of the Southern African Development Community (SADC).

Multilateral policy development on data protection: the EU and Africa

The EU [adopted the GDPR](#) in 2016, replacing the 1995 Data Protection Directive. It came into full implementation by member states in 2018, and has since come to be considered, despite its flaws, as the [gold standard](#) for data protection.

The GDPR created a binding regulation for all member states, harmonizing previously fragmented law and practice across the EU. It also had a ripple effect: the regulation's third-party provisions extended compliance requirements to any non-EU countries and others who wanted to continue trading with the bloc. Because Europe is Africa's largest trading partner, that requirement for compliance has led to the [exportation of these privacy norms](#) to Africa.

But the ideal of [global compliance](#) assumes that concerns related to privacy and data protection are similar across contexts. The result has been data-protection laws across Africa that are in various stages of development, with a greater focus on alignment with the GDPR than on needs based on the local context.

Europe began setting the standards for data protection even prior to the GDPR. That influence and support is evident in the evolution of data-protection frameworks in regional bodies ranging from the African Union to SADC, an intergovernmental organization of 16 states that aims to advance sustainable and equitable economic growth and socio-economic development.¹ The project of [Support for Harmonization of the ICT Policies in Sub-Saharan Africa](#), funded by the European Commission and the International Telecommunications Union (ITU), launched in 2008. It was intended to support creation of the necessary policy, legal, and regulatory frameworks for ICT infrastructure in the region, "using coordinated approaches that respond to the needs of countries in a comprehensive and cost effective manner." The program was chaired by the African Union and supported

1 SADC Member States: Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini (formerly Swaziland), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe; See SADC website at <https://www.sadc.int/member-states/>

by the continent's Regional Economic Communities, which group countries for economic integration. The SADC model law on data protection was developed in this context in 2012, with the guidance and support of consultants to the SADC secretariat, working with the [Communications Regulators Association of Southern Africa \(CRASA\)](#).

In addition to being developed with support from the EU, the SADC model law was [strongly influenced](#) by innovative views in the first drafts of the EU's GDPR. The SADC government ministers responsible for telecommunications, postal services, and ICT adopted the model law at their meeting in Mauritius in November 2012. While it is non-binding, its relevance lies in its role as a reference for countries developing their own national laws. Currently in the SADC region, [seven countries have data-protection laws](#) at various stages of implementation: Angola, Lesotho, Madagascar, Mauritius, Seychelles, and South Africa – and Zimbabwe only for its public sector. Zambia, Tanzania, Eswatini (formerly Swaziland), and Zimbabwe currently have legislation pending.

Feminist framework

From a feminist perspective, the concern with the internet is that it reinforces power dynamics that increase the marginalization of women and gender-diverse groups. The internet and digital platforms serve as a means to connect and shift patriarchal norms and practices. Therefore, there is a need to understand the intersection of gender and data. The collection, processing, use, and dissemination of data takes place amid existing structural inequalities that raise the risk of [surveillance, violence, and other human rights violations](#). Various actors have used [surveillance](#) as a tool to control women, gender-diverse people, and sexual expression when something does not fit into the hetero-patriarchal norm. Privacy breaches increase the vulnerability of women and gender-diverse people, as their private data is found online and is used to track and monitor them.

Increased access to data also may result in online gender-based violence, as personal data is used to harass and wage attacks. Content moderation and self-censorship of women and gender-diverse people increases the risk that they will be censored more than others when they go against the norm, as their activities may be deemed to violate platform and social community standards. In addition [bias and discrimination](#) for marginalized groups is also experienced with algorithms often being used to support decision making, at the intersection of issues such as race, gender, ethnicity, class, and geolocation. For example, women, [in particular women of color, are being denied](#) access to finance due to algorithms built on historical discriminatory data that excluded women and did not factor in race.

A feminist perspective applied to data protection allows clear analysis of whether these issues are taken into consideration and development of recommendations that will not be simply a “one size fits all” approach, even within multilateral contexts. The [Feminist Principles of the Internet](#), first drafted at a 2014 meeting in Malaysia of the Association for Progressive Communications and most recently published in a new version in 2016, provide a guiding framework for thinking of a transformative internet that supports the right to

privacy and to full control over one's own personal data and information online. The 17 principles cover issues related to access, movements, economy, expression, and embodiment. Fundamentally, the privacy and data principle, encourages a move away from the idea that data is simply something used for profit and to manipulate behavior, and toward a recognition of the surveillance risks, particularly for women and gender-diverse people.

Protecting data related to gender and sexuality

Data related to sexual topics or sexual orientation is especially sensitive and must be treated with extra security when collecting, processing, using, and disseminating it. The GDPR recognizes data related to sex life and sexual orientation as special categories, whereas the SADC model law recognizes gender and sex life data as sensitive data.

However, most data-protection legislation **does not recognize gender** as a sensitive or special category. The SADC model law is an example of the exception. **Gender** is a social and cultural construct of what it means to identify as a man, woman, or non-binary person, and sexual orientation describes the genders that a person is attracted to.² The construct of gender allows us to understand the approach to data collection, processing, and use on individuals and communities within particular social contexts. **Not recognizing gender** in data protection leaves room to overlook related harms and nuances in how gender constructs shapes the experience of data collection and processing and the protections needed. For example, there have been cases of **women being stalked** after leaving personal details for contact tracing as part of Covid-19 measures. By recognizing gender, the SADC model law acknowledges the potential unlawful or arbitrary discrimination based on gender. However, its approach to gender focuses on the binary man or women, which excludes gender-diverse people. The absence of gender from frameworks such as the GDPR overlooks the context of social constructs related to gender that shape experiences of privacy and data protection.

Likewise, protecting data related to sexual life and sexual orientation upholds one's right to privacy to determine who has information about their life. When such data is collected and used, safeguards must be applied to maintain this privacy. Boston University Law School Professor Danielle K. Citron **highlights** that sexual privacy is important to allow for an individual to have agency over sexual determination and intimacy. Women and gender-diverse people from marginalized communities often experience more significant repercussions when their sexual privacy is invaded. As highlighted in the aforementioned Feminist Principles and in work on surveillance, women and gender-diverse people are particularly

² The applied definitions are from Pocket Queerpedia by the Tshisimani Centre for Activist Education. The purpose of this glossary is for activist to broaden their understanding of the work and how gender and sexuality shape this world. <https://www.genderdynamix.org.za/for-educators>

diminished in contexts where patriarchal norms consider them as subordinate. So it is particularly important to dismantle this kind of dynamic by recognizing the role of gender and sexuality in data protection/privacy.

However, there are exemptions to the processing of special and sensitive categories of data. Processing this category of personal data is a feminist issue because the point of contention is whether the safeguards are adequate to ensure privacy in a way that does not result in surveillance. It should also recognize the context, power dynamics that allow for the collection and processing of this data and how it will be used – to ensure it does not lead to harm.

A key element to consider in relation to socio-political or sexual autonomy and freedom for women and gender-diverse people is [consent](#). After all, [data essentially is an extension of people](#), and people need to have agency in deciding how their data is used. But availability of consent is undermined by a common assumption that, in the act of clicking yes or no, users are somehow equal in terms of their power and understanding of the technology, even though we know that historical and sociological factors inevitably come into play. Similarly to [cases of sexual assault](#) or to cases where the user is [deemed to have less social standing](#) based on class, gender or economic standing, the individual may not believe they are in a position to say no.

In both the GDPR and SADC model law, processing of this data is possible when consent has been given. Both laws make an exception that Union or Member state law may override consent if there is a prohibition to process this data. SADC further goes on to state the need for consent in writing. Consent is assumed as being freely given by the data subject, and that the consent is specific, informed, and unambiguous through a statement or clear affirmative action in the processing of their data. [Feminist values](#) related to the body and the concept of consent shed light on the shortcomings in these regulations – for example, that consent is an ongoing process; that it must be mutual and sincere; that it should be based on equal power and freedom to act; and that it considers historical/sociological structures and is adapted to contextual situations. The concept of consent, across all processing of data, must be handled with the recognition that, while it assumes an individual's ability to decide, that capacity is determined by social context, and in some cases, one may not have the option to say no. Vulnerable groups in need of assistance [may not have the ability to say no to having their data collected](#) when that data determines access to social grants. The result is often the unauthorized use and exploitation of social grants recipients' data as in the case of [South African Social Services Agency \(Sassa\) and Cash Paymaster Services \(CPS\)](#).

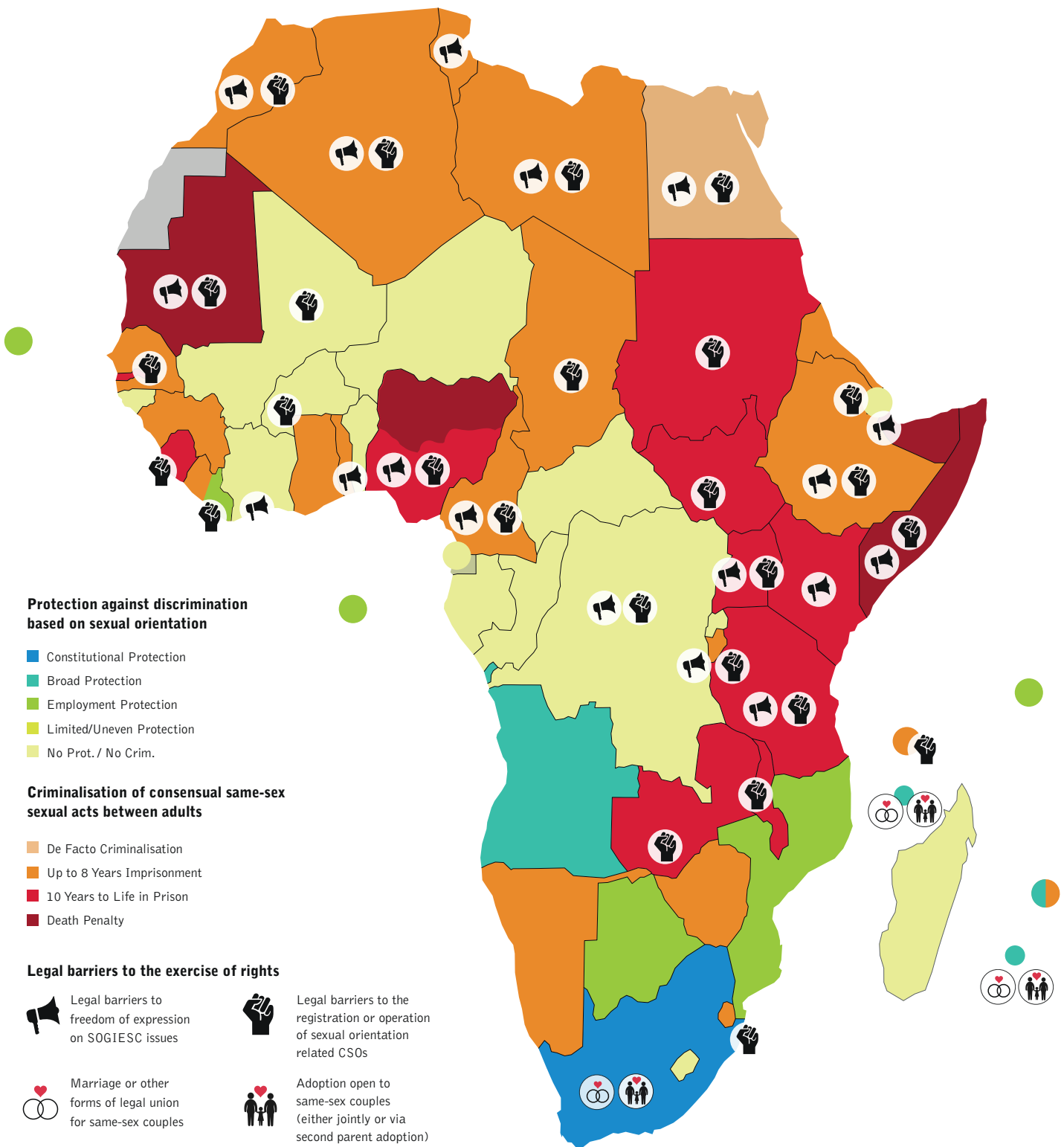
In the SADC model law, the grounds for processing sensitive data other than consent are particularly concerning. Part V Section 15 (4) is particularly concerning as sex life data could be processed for "the evaluation, guidance and treatment of persons whose sexual conduct can be qualified as an offence, and who has (sic) been recognized and subsidized for the achievement of that objective by the competent public body for such processing." The wording in this document is a result of regional stakeholder consultations and negotiations. In a context in which the sexual lives of gender- and sexual minorities are considered deviant by law and can qualify as an offense, the idea that institutions could access or process their data is alarming and disregards the human rights of all people, regardless of their sex

lives. This could apply in cases of homosexuality, sex work, and sexual expressions that may be considered obscene or morally corrupting.

Only 22 African countries have legalized homosexuality. In some countries, sex work is illegal and public-disorder laws are used to criminalize it. In Malawi, Zambia, and Lesotho, having and distributing sexualized or nude images may be prosecuted as cases of obscenity. In the SADC region, Angola, South Africa, Botswana, Mozambique, Lesotho, and the Seychelles have laws that protect the rights of gender-diverse individuals. However, Namibia, Eswatini, Malawi, Tanzania, and Zimbabwe criminalize certain sex acts in ways designed to suppress certain groups. Even where homosexuality is protected by law, homophobia and transphobia sometimes result in privacy breaches and even the killing of queer individuals. Furthermore, there is no clarity on what “guidance and treatment” means in the SADC model law, making this a broad and problematic basis for data-privacy exemptions. In other words, the protection of basic dignity in the collection and use of such data is not recognized in the “evaluation, guidance and treatment” clause at all.³

3 This review is also expanded in a forthcoming publication by the author on “Privacy and data protection – challenges and prospects? Gendered digital inequalities – how do we ensure gender transformative law and practice in the age of AI in Africa?”.

Graphic: Laws regarding same-sex sexuality in Africa



Source: State-Sponsored Homophobia, an ILGA report by Lucas Ramon Mendos, Kellyn Botha, Rafael Carrano Lelis, Enrique Lopez de la Peña, R.I. and Daron Tan

As sex work or aspects of it also are criminalized, the SADC clause on processing data related to sexual conduct that is considered a legal offense leaves sex workers vulnerable to having their information stored and processed online for the same purposes of “evaluation, guidance and treatment.” The [movement to decriminalize](#) sex work emphasizes respect for the human rights of such workers and the imperative that they be protected from violence, intimidation, and harassment from clients, partners, and instruments of the State such as the police. If the SADC model law provision is implemented at a national level, it could lead to seizure of online platforms and digital resources used by sex workers. One example of such an instance was the [“Redbook case” in 2014](#), when U.S. federal law enforcement authorities seized the digital information of an online community of sex workers in what the officials said was an investigation into prostitution and money laundering, even though at least some – possibly many – of those whose privacy was invaded had nothing to do with the alleged crimes. Additionally, obscenity laws raise issues related to intimate images that may have been taken with consent but distributed without permission. Victims of such distribution may [be liable to a fine or face imprisonment](#) or [seen as](#) requiring treatment to “correct” a behavior.

Recommendations for safeguarding sexuality and gender data

The [intersection of gender and data](#) is often treated a secondary consideration in data protection, yet the complex impact on society requires that this issue becomes a primary concern. Gender perspectives must be integrated into all work, from policy and regulation development to implementation, highlighting where all stakeholders can play a role. The collection, processing, and use of special or sensitive categories of data are likely to have gender-specific harms unless principles and actions cognizant of the context are put into place. Through a [feminist lens](#), data-protection standards must account for the risks of State or company surveillance and for potential harms stemming from cultural and family contexts. Especially with large amounts of data being used for development of AI-based solutions, there is a need to ensure data protection [also responds to harms](#) that emerge with the processing of all data – not just personal data – in relation to gender and sexuality. Implicit and unconscious bias and discrimination must also be recognized in the collection, processing, and use of data on sexual life styles, sexual orientation, and gendered practices within patriarchal contexts especially when there are legal ramifications. The [U.N. Special Rapporteur on the Right to Privacy](#) noted that non-discrimination is paramount to avoiding inequality, injustice, and suffering that has the potential to affect the enjoyment of human rights.

One possible starting point for refining the approach to issues of gender and sexuality in data protection is the [Yogyakarta Principles \(YP\)](#). Developed by experts from the U.N., academia, and other institutions and named after an Indonesian city where some of their development took place in 2006, these 29 principles seek to elaborate how international

human rights law applies to issues of sexual orientation and gender identity. Principle 6 specifically refers to ensuring privacy regardless of sexual orientation and gender identity. The YP Plus-10, adopted in 2017, provided an additional update to Principle 6, including that such requirements of processing respect all persons' right to self-determination. The principles highlight the importance of ensuring gender is considered within privacy by respecting the right to self-determination and advocating for the repeal of laws that may criminalize groups based on their sexuality. This is an important right that needs to be accounted for within the SADC model law on data protection, as even within the [African Charter on Human and Peoples' Rights](#), self-determination is maintained as a right. Applying laws on data processing and protection in ways that are based in the Yogyakarta Principles would bring in the gender perspective and nuance to analyze whether the processing is being done by mutual consent, considers the social and historical context, and allows users to say no without repercussions. As a result, users would retain control over data and avoid the harms of surveillance.

The [U.N. Special Rapporteur on the Right to Privacy](#) also provides guidelines in relation to data on gender and sexuality. The recommendations highlight a need for robust data-protection laws that take gender differences into account, as well as mechanisms for assessing gendered issues, and public awareness campaigns. The rapporteur cited the need to engage the public in developing policies relating to terminology, definitions, and special categories associated with intersex, transgender and gender-diverse communities. Neither the GDPR nor the SADC model law provided definitions of sexual life, orientation, or gender.

There is also a [need to build public rights awareness](#) among women and gender-diverse people. This requires data-protection authorities to engage with gender-justice activists in developing gender-responsive public awareness campaigns and in designing monitoring programs for gender and sexuality issues raised in complaints. [It is important to have](#) measures that guarantee confidentiality of personal data of individuals who are vulnerable due to their gender and sexuality. Among the concrete steps in this regard would be vulnerability assessments of information systems and regular training for staff on data privacy and security. Lastly, privacy impact assessments and other mechanisms could ensure that data analytics do not result in inferences about individuals or groups, leading to discrimination. The Special Rapporteur encourages States to develop data-protection standards that allow for all individuals, regardless of gender, to have control over their personal information, especially with regard to data on gender and sexuality.

Accountability mechanisms must go beyond government and private entities. It is important to ensure that [civil society organizations and academic communities](#) are engaged, even within multilateral systems based on State membership, to ensure accountability and transparency. At the time of writing this paper, I had not come across a gendered analysis of the SADC model law, which highlights the failure to consider such perspectives and issues and affirms the need for more engagement from gender-justice experts. The African Declaration of Internet Rights and Freedoms developed a [Privacy and Personal Data Protection Advocacy toolkit](#) which calls for gender-justice activists to be part of the data-protection discourse. They could contribute gender-related analysis on the right to privacy; build awareness about

the intersection of gender and data; and work towards comprehensive monitoring of privacy breaches related to sex, sexuality, gender, and gender expression. In addition, a system should be established to collect evidence about user experiences with data collection, processing, and use in relation to gender and sexuality.

Conclusion

The multilateral discourse on data protection has focused on ensuring harmonization of laws, as in the case of the EU's GDPR setting the standard and the African region trying to comply with perceived global standards to ensure continuous economic engagement. The Feminist Principles work towards ensuring all rights of people are protected and provides grounds for creating special categories of data – in particular, data related to sexuality and sexual orientation.

The recommendations presented in this paper, drawn from multistakeholder discourse, highlight the need to assess the impact of data protection from a gender perspective. The gaps in both the GDPR and the SADC model law highlight the need for a responsive approach to considering gender and sexuality in data protection. The feminist approach to reviewing the exemptions of processing sensitive or special categories of data highlights the need to take into context the power dynamics in relation to marginalized groups as well as to determine whether the way consent is framed is sufficient to not result in harms.

References

- Access Now. (2020, May). *GDPR: Three years in, and its future and success are still up in the air*. Retrieved from <https://www.accessnow.org/gdpr-three-years/>
- African Union. (n.d.). *Africa EU Partnership*. Retrieved from Harmonising telecommunications: <https://africa-eu-partnership.org/en/success-stories/harmonising-telecommunications>
- African Union. (1986). *African Charter on Human and Peoples' Rights – Banjul Decl.* Retrieved from <https://www.achpr.org/legalinstruments/detail?id=49>
- African Declaration on Internet Rights and Freedoms Coalition. (2021). *Privacy and Personal Data Protection in Africa – Advocacy Toolkit*. Retrieved from <https://africaninternetrights.org/en/node/2558>
- Alt Advisory. (2021). *Data Protection Africa*. Retrieved from <https://dataprotection.africa/>
- Association for Progressive Communication. (2018). *Gender perspectives on privacy: Submission to the United Nations Special Rapporteur on the right to privacy*. Retrieved from <https://www.apc.org/en/pubs/gender-perspectives-privacy-submission-united-nations-special-rapporteur-right-privacy>
- Bernardo Fico, G. S. (2021, March). *Does Brazil's LGPD recognize gender identity, sexual orientation as sensitive personal data?* Retrieved from IAPP: <https://iapp.org/news/a/does-brazils-lgpd-recognize-gender-identity-and-sexual-orientation-as-sensitive-personal-data/>
- Chair, C. (2020). *MY DATA RIGHTS: Feminist Reading of the Right to Privacy and Data Protection in the age of AI*. Retrieved from [my data rights: https://mydatarights.africa/policy-recommendations/](https://mydatarights.africa/policy-recommendations/)
- Citron, D. K. (2019). Why Sexual Privacy Matters for Trust. *96 Washington University Law Review* 118.
- Computers, Privacy and Data Protection. (2018). *Gendered Data Bodies*. Retrieved from https://www.youtube.com/watch?v=F92_KzzK8N4
- Cottier, G. G. (2020). Comparing African Data Privacy Laws: International, African and Regional Commitments. *University of New South Wales Law Research Series*.
- European Data Protection Supervies. (n.d.). *The History of the General Data Protection Regulation*. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
- Feminist Internet. (n.d.). *Feminist Principles of the Internet*. Retrieved from <https://feministinternet.org/en/principle/privacy-data>

Hernández, Y. P. (2016). Consentimiento sexual. *Revista Mexicana de Sociología* Vol. 78, No. 4 , 741-767.

Internet Society. (2018). *Personal Data Protection Guidelines for Africa* A joint initiative of the Internet Society and the Commission of the African Union. Retrieved from Internet Society: https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

ITU. (2013). *Establishment of Harmonized Policies for the ICT Market in the ACP Countries* Data Protection: Southern African Development Community (SADC) Model Law. Retrieved from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

Kirya, S. Chisala Templehoff. (2016). Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda. *Palgrave Communications* volume 2, Article number: 16069.

Makulilo, A. (2021). The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius. *The International Journal of Human Rights* Volume 25 – Issue 1: *The right to privacy in the digital age: different perspectives around the globe* , 117-146.

Kovacs, A. (2017). *Gendering Surveillance*. Retrieved from Internet Democracy: <https://genderingsurveillance.internetdemocracy.in/>

Pena P and Varon J. (2019). *Consent to our Data Bodies* lessons from feminist theories to enforce data protection.

Privacy International. (2018, September). *Privacy International's submission on the consultation Gender perspectives on privacy*. Retrieved from https://privacyinternational.org/sites/default/files/2018-11/PI%20submission%20on%20gender%20consultation_September%202018.pdf

Sidiropoulos, E. (2019, November). *The retreat of multilateralism: What should Africa do?* Retrieved from <https://saiaa.org.za/research/the-retreat-of-multilateralism-what-should-africa-do/>

Special issue on "feminist data protection". (2020, June). Retrieved from Internet Policy Review: <https://policyreview.info/node/1470>

The Citizen. "Black Sash back in court over social grants" (2018) <https://citizen.co.za/news/1845959/black-sash-back-in-court-over-social-grants/>

Vatanparast, R. (2020). Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy. *80(4) Heidelberg Journal of International Law*, 819-845.

Wang, T. (2020, August). *You are not your data but your data is still you*. Retrieved from Deep Dives: <https://deepdives.in/you-are-not-your-data-but-your-data-is-still-you-b41d2478ece2>

United Nations. (2020). *Report of the Special Rapporteur on the right to privacy*. Retrieved from Human Rights Council: <https://undocs.org/A/HRC/43/52>

Yogyakarta Principles. (n.d.). *The Yogyakarta Principles plus 10*. Retrieved from <http://yogyakartaprinciples.org/principles-en/about-the-yogyakarta-principles/>

Imprint

Heinrich-Böll-Stiftung European Union, Brussels, Rue du Luxembourg 47-51,
1050 Brussels, Belgium

Heinrich-Böll-Stiftung Washington, DC, 1432 K St NW, Washington, DC 20005, USA

Contacts, Heinrich-Böll-Stiftung European Union

Anna Schwarz, Head of Program, Global Transformation,
Heinrich-Böll-Stiftung European Union, Brussels,

E Anna.Schwarz@eu.boell.org

Lisa Tostado, Head of Program, Climate, Trade and Agricultural Policy,
Heinrich-Böll-Stiftung European Union, Brussels,

E Lisa.Tostado@eu.boell.org

Contacts, Heinrich-Böll-Stiftung Washington, DC

Sabine Muscat, Program Director, Technology and Digital Policy,
Heinrich-Böll-Stiftung Washington, DC,

E Sabine.Muscat@us.boell.org

Liane Schalatek, Associate Director, Heinrich-Böll-Stiftung Washington, DC,

E Liane.Schalatek@us.boell.org

Christin Schweisgut, Program Director, Infrastructure and Development,
Heinrich-Böll-Stiftung Washington, DC,

E Christin.Schweisgut@us.boell.org

Place of publication: <https://us.boell.org/> | <http://eu.boell.org>

Release date: July 2021

Editor: Viola Gienger, Washington, DC

Illustrations: Pia Danner, p*zwe, Hannover

Layout: Micheline Gutman, Brussels

License: Creative Commons (CC BY-NC-ND 4.0),
<https://creativecommons.org/licenses/by-nc-nd/4.0>

The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the Heinrich-Böll-Stiftung Washington, DC and Heinrich-Böll-Stiftung European Union, Brussels.