Concern without Consensus: Addressing the Digital Divide in Legislation for Privacy and Data Protection in Africa.

Felix Onan-Olindi[1]

Abstract

As the Fourth Industrial Revolution (4IR) reshapes economies, the rapid adoption of technologies such as Artificial Intelligence, (AI), data analytics, and the Internet of Things brings a plethora of challenges for lawmakers. In Africa, the digital divide has exacerbated these challenges and complicated efforts to legislate effectively for privacy, data protection, and digital rights. While these emerging technologies present opportunities, the gap between those with digital access and those without risks deepening existing inequalities. This paper examines the complexities of legislating in contexts where not all citizens experience the benefits of 4IR, and also makes a case for the need for inclusive, future-proofed privacy and data protection laws. It also proposes a framework for African lawmakers that ensures legislation efforts are both protective and inclusive while considering the continent's unique socio-economic realities.

Keywords: Digital Divide; Fourth Industrial Revolution; Artificial Intelligence; Digital Rights; Privacy; Data Protection Legislation

1. Introduction

Mama Marriam, lives in a rural village in Sironko district, Uganda. One afternoon, she sat on the grass patch of her compound as she came to terms with her frustration when her basic smartphone displayed the dreaded "*No Network*" message. She had thought of investing in a small business of reselling sweet bananas (*bogoya)* which was readily available here. She had hoped to sell these bananas in Kampala regularly, and was convinced that digital platforms would connect her to larger markets in Kampala and beyond. However, the absence of reliable internet made this dream seem impossible. Her village, like many others across Africa, are a world away from the digital advancements promised by the 4IR. Meanwhile in Kampala, Nicholas, a software engineer is working on a cutting-edge digital product for a major tech firm. As his career thrives in a tech-driven economy, my mother's business has stagnated. This difference between their experiences was not just geographical, it is emblematic of Africa's widening digital divide.

The Fourth Industrial Revolution (4IR) has introduced a paradigm shift in technology, largely driven by advancements in AI machine learning, Internet of Things and data analytics. These innovations present opportunities for development in economies, healthcare, education and governance. However, in Africa, where a significant portion of the population lacks access to digital technologies, the digital divide hinders the efficacy and relevance of privacy and data protection legislation.

Despite global strides toward digital inclusion—with the worldwide average for regular internet access standing at 67%—Africa lags significantly behind. In Africa only 37 percent of the population were

[1] Final Year Law Student, Makerere University.

internet users in 2023, compared with a global average of 67 percent.[2] This digital divide leaves a substantial portion of the continent's population disconnected from the digital economy and vulnerable to exclusion. The absence of internet access not only limits economic participation but also marginalises these individuals in policy and legislative discussions related to the digital economy.[3] A dangerous misconception prevails: because these communities are not actively engaged in the digital sphere, they are seen as unaffected by digital policies and regulations. This fallacy overlooks the indirect impact that digital economy legislation can have on socio-economic opportunities, governance, and service delivery for those left offline.[4]

The digital economy therefore creates a paradox. While it presents great opportunities, the gap between those who have access and those who do not is widening, and this disparity raises questions about the relevance, efficacy and inclusivity of laws crafted without a broad consensus or consideration of the realities of digital inequality. How do you legislate for a future where not everyone is connected to the present? How do you ensure that privacy and data protection laws safeguard both the tech-savvy professional in Kampala and the entrepreneur like *Mama Marriam*, struggling with basic connectivity? Without concerted efforts to ensure inclusivity in legislative processes, there is, and has been a risk that data protection and privacy laws will be disconnected from the realities of a digitally marginalised population.

This paper explores how policymakers and legislators on the African continent can craft privacy and data protection laws that are future-proofed for the 4IR while addressing the existing digital divide and taking into consideration the lived realities of millions of Africans who, like *Mama Marriam*, are still waiting to be connected to the digital revolution.

2. Understanding the Digital Divide.

The concept of the digital divide has been discussed by scholars, particularly in the context of the growing reliance on the internet for various societal functions. Manuel Castells defines the digital divide as the "inequality of access to the internet," and emphasises that access to the internet is essential for overcoming inequality in a society increasingly organised around it. Castells posits that in a world where dominant social functions are structured online, lack of internet access can deepen existing social and economic disparities between individuals and communities.[5]

Similarly, Jan van Dijk, another leading theorist in the network society, describes the digital divide as "the gap between those who do and do not have access to computers and the internet".[6] Van Dijk's definition extends beyond mere internet access, and focuses on the broader scope of technological inequalities that inhibit individuals from fully participating in a digitally driven society. Without access

[2] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2022* (Geneva: ITU, 2022), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2022.pdf.

[3] R. Evangelista, P. Guerrieri and V. Meliciani. "The economic impact of digital technologies in Europe." Economics of Innovation and New Technology, 23 (2014): 802 - 824.

[4] Rumana Bukht and Richard Heeks. "Digital Economy Policy in Developing Countries." (2018).

[5] Manuel Castell, *The Internet Galaxy: Reflections on the Internet, Business and Society* (Oxford University Press 2002) 248.

[6] Jan van Dijk, *The Network Society. Social Aspects of New Media (2nd edn, Sage Publications 2006) 178.*

to essential digital tools and technologies, people are effectively excluded from the opportunities that the digital economy offers.

Other scholars, such as Pippa Norris, expand this definition and argue that the digital divide encompasses "any and every disparity within the online community."[7] This interpretation considers not only physical access to the internet but also disparities in digital literacy, usage patterns, and the ability to meaningfully engage in with online resources. Ernest J. Wilson III further elaborates on this idea, and defines the digital divide as an "inequality in access, distribution, and use of information and communication technologies between two or more populations."[8] Wilson's perspective takes into consideration the importance of access to digital infrastructure and the need to address imbalances in how the technologies are distributed and utilised across different segments of society.

3. Africa and the Digital Divide

The exclusion in digital access in Africa is not merely about access to technology but represents a broader socioeconomic and legislative challenge. Scholars such as Manuel Castells have highlighted how the global network society is developing in parallel, with those connected to the internet enjoying substantial advantages over those who are excluded. In this regard, access to the internet is seen as essential for overcoming broader inequalities.[9] The lack of such access in Africa, creates a segmented society, which, according to theorists like Jan van Dijk, perpetuates disparities in education, income and social participation.[10] This phenomenon must be seen in the context of privacy, digital rights and data protection, where African countries are particularly vulnerable due to their limited digital awareness and infrastructure.

In many ways, the digital divide could also be viewed as a form of "digital apartheid", where certain groups are systematically excluded from the cyberspace and the benefits it offers.[11] This exclusion is rooted in real-world issues such as poverty, unequal resource distribution and a lack of investment in digital infrastructure. For instance, data from the United Nations Human Development Report (UNHDR) highlights that 16 out of 20 African countries with internet access rates below 1% are also ranked among the least developed countries in the world.[12] The correlation between low Human Development Index (HDi) scores and limited internet access makes the case for how limited internet access underscores how global social gaps mirror the digital divide. In these countries, fundamental needs such as food, water, and healthcare often take precedence over technological advancements, thereby creating a vicious cycle of the digital divide.

---

[7] Pippa Norris, Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide (Cambridge University Press 2001) 4.

[8] Slavka Antonova and Ernest J. Wilson, "St Antony's International Review," 3, no. 1 (2007): 99–101.

[9] *Ibid.*

[10] *Ibid.*

[11] Christian Fuchs, "Towards a Critical Theory of Cyberspace" (2005) 2 Journal of Information, Communication and Ethics in Society 64, 68.

[12] United Nations, Human Development Report (2020)

Ted Turner, founder of CNN, noted that discussions around the digital divide must be framed within the context of basic human needs, as many individuals in the developing world struggle with challenges far more pressing than internet access.[13] This therefore reflects the broader dilemma that African governments and policymakers face: how to prioritise digital and privacy legislation when portions of the population still lack access to basic necessities.

4. Gender, Rural-Urban and Class Divides in Access

The digital divide is not just a class issue. It also reflects deeper social and economic inequalities. For instance, the gender digital divide is a well-documented issue, with women in Africa being significantly less likely to have access to smartphones and the internet compared to men.[14] In Sub-Saharan Africa, 14% of women are less likely to own a basic mobile phone, and 34% are less likely to own a smartphone.[15]

Similarly, there is a notable rural-urban divide in digital access. In Southern Africa, rural populations are far less likely to have internet access compared to their urban counterparts.[16] This divide is most stark in countries like Malawi, where 9.3% of rural residents have internet access compared to 40.7% of urban residents.[17] Such disparities necessitate the adoption of intersectional approaches to legislating digital rights and privacy. The rural-urban divide, coupled with class-based inequalities, means that laws designed to protect digital privacy and data rights must take into account all the unique needs of African populations.

5. Privacy and Data Protection in the 4IR: The African Context

In recent years, African states have taken steps towards adopting and implementing data protection and privacy legislation.[18] This has been partly in response to global trends on personal data protection in light of the growth in digital technologies and the Fourth Industrial Revolution (4IR). Regardless, challenges in enforcement and compliance with International Human Rights standards persist.[19]

As of 2022, 61% of African States had enacted data protection and privacy laws. Countries have gone an extra mile to either pass or update their legislation to safeguard citizens' privacy and data.[20]

At the regional level, Africa has adopted several frameworks aimed at guiding member states in enacting privacy and data protection legislation. The *African Charter on Human and Peoples Rights*

---

[13] Ted Turner, as quoted in *The UN World Economic and Social Survey (2005) 84.*

[14] GSMA, the Mobile Gender Gap Report (2020) 14

[15] Ibid.

[16] International Telecommunication Union (ITU), "Measuring Digital Development: Facts and Figures" (2021).

[17] Ibid.

[18] Boshe, P., Hennemann, M., & Meding, R. (2022). African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward. Global Privacy Law Review.

[19] Alex B. Makulilo. "Data Protection Regimes in Africa: too far from the European 'adequacy' standard?." International Data Privacy Law, 3 (2013): 42-50.

[20] Greenleaf, G., & Cottier, B. (2020). Comparing African Data Privacy Laws: International, African and Regional Commitments.

(ACHPR), the continent's primary human rights instrument does not explicitly mention the right to privacy. However, it has been argued that privacy is implicitly protected through other rights enunciated in the Charter for example the right to dignity[21] and freedom of expression.[22]

The ACHPR's *2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa* adopts a progressive stance by outlining specific provisions on privacy and personal data protection. Principle 40 recognises the Right to Privacy and Personal Information and asserts that every individual has a right to privacy, including the protection of personal information and communication confidentiality. Principle 42 urges member states to adopt laws that protect personal information in line with international human rights standards and ensure that individuals have control over how their data is processed.[23]

The *Malabo Convention on CyberSecurity and Personal Data Protection* encourages members to adopt comprehensive laws on data protection and establish national Data Protection Authorities. However, the Malabo Convention has faced criticism over its vague provisions, such as criminalising "insulting language." As of July 2024, the Convention still lacked the necessary ratifications to enter into force.[24]

6. The Intersection of Data Protection and Digital Divide

In Europe, data protection laws, notably the General Data Protection Regulation (GDPR), are designed to protect individual privacy by regulating the processing of personal data.[25] These regulatory frameworks are predicated on the assumption of a relatively uniform digital environment, where data subjects are both abundant and digitally literate. The GDPR, for instance, defines 'personal data' as "any information relating to an identified or identifiable natural person," thus interlinking privacy protection with data processing practices[26]. While this definition is thorough and aligns well with European digital practices, it fails to address the stark contrasts found in regions like Africa, where a significant portion of the population is excluded from the digital realm.

The transition from the 1973 Council of Europe's resolution on data protection to the GDPR has established a precedent where 'data' and 'information' are used interchangeably in legal discourse.[27] This conflation has global ramifications, particularly for regions where the digital infrastructure and literacy rates diverge markedly from those in Europe. In Africa, the legal treatment of 'data' as

[21] African Union, *African Charter on Human and Peoples' Rights*, art. 5.
[22] African Union, *African Charter on Human and Peoples' Rights*, art. 9.
[23] African Union, *African Charter on Human and Peoples' Rights*, art. 5.
[24] African Union, *Malabo Convention on Cyber Security and Personal Data Protection*, adopted June 27, 2014, not yet in force as of July 2024.
[25]"The EU General Data Protection Regulation (GDPR)." (2020).
[26] European Parliament and Council of the European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 27 April 2016, Article 4(1).
[27] Council of Europe, Resolution (73) 22 on the Protection of the Privacy of Individuals with Regard to Automatic Processing of Personal Data, 26 January 1973.

synonymous with 'information' overlooks the specific challenges of digital exclusion and infrastructural deficiencies.[28]

In Africa, the practical realities of data collection and usage diverge significantly from those in more digitally developed regions.[29] The GDPR's framework, which assumes a level of digital engagement and data subject participation that is not universally present, fails to accommodate the complexities of the digital divide. In many African contexts, where internet access is sporadic and digital literacy is limited, the concept of personal data protection becomes complex and often impractical. For example, the widespread digital exclusion means that large segments of the population are not engaged in the digital economy, and thus, do not benefit from or are not protected by these data protection laws.[30]

The assumption embedded in European data protection laws that data subjects have equal access to digital resources is flawed when applied globally. In Africa, where data processing systems may be rudimentary or non-existent, the GDPR's emphasis on personal data protection does not necessarily translate into meaningful privacy safeguards for those who are not digitally included. The notion that data can be uniformly protected overlooks the socio-economic factors that inhibit digital access and literacy, which are critical to understanding and applying data protection effectively in the African context.[31]

This legal construction of data protection, grounded in the assumption of a universal digital environment, fails to address the unique challenges posed by Africa's digital divide. In areas where internet access is limited or non-existent, the legal protections designed to safeguard personal data and privacy are rendered ineffective.[32] For example, rural communities that lack reliable internet connectivity cannot benefit from these protections, nor can they engage with the digital services that require the processing of personal data.[33]

Additionally, the conflation of data and information in legal frameworks fails to address the broader implications of digital exclusion. In regions with uneven digital development, data protection laws designed for a digital ecosystem where data and information are readily accessible may inadvertently exacerbate the digital divide. This is particularly relevant when considering automated decision-making processes that rely on comprehensive and accurate data, which may be skewed or incomplete due to

---

[28] Efe Lawrence-Ogbeide, Chiemeka Felix Nwosu and Olumide Babalola. "A Value Assessment of Personal Data: Towards Greater Privacy Consciousness in Africa." International Journal of Law and Society (2023).

[29] Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. Michigan Journal of Race & Law.

[30] European Parliament and Council of the European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 27 April 2016, Article 4(1).

[31] Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order," *International and Comparative Law Quarterly* 63, no. 3 (2014): 569–597.

[32] Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. Michigan Journal of Race & Law.

[33] Hollman, A., Obermier, T., Burger, P., & Spanier, A. (2020). Rural Measures: A Quantitative Study of The Rural Digital Divide. Journal of Information Policy.

limited digital participation. Such disparities highlight the need for a more nuanced approach to data protection that considers the varying levels of digital engagement across different regions.[34]

7. Proposed Framework for Privacy and Data Protection Legislation in Africa

The inadequacies of current data protection frameworks in addressing the African context necessitate a reimagining of privacy and data protection legislation that is not merely transplanted from European models but is tailored to the unique socio-economic, infrastructural, and digital realities of the continent. An effective legal framework for Africa must go beyond the reactive approach of safeguarding individual privacy and actively seek to close the digital divide. This requires a holistic vision that integrates digital inclusion into the very fabric of data protection laws.[35]

One foundational principle for such a framework must be contextual relevance.[36] While international norms like the GDPR offer valuable guidance on the principles of data protection—such as consent, transparency, and accountability—their applicability to Africa must be re-evaluated. A framework tailored for Africa should explicitly recognize the socio-economic conditions that inhibit digital access for large segments of the population. For instance, it should include provisions that focus on building digital literacy and access as preconditions for equitable data protection. As Eltis suggests, privacy rights must be seen not only as protections from exploitation but also as empowering mechanisms that enable broader participation in digital society.[37] In this view, privacy protections should serve to level the playing field by ensuring that all individuals can meaningfully engage with digital systems.

Furthermore, a rights-based approach to data protection in Africa must focus on the intersection of digital rights and socio-economic rights.[38] African nations must acknowledge that the digital divide is deeply intertwined with economic inequalities and must legislate accordingly. This approach requires recognising access to digital infrastructure as a right in itself, without which the enforcement of privacy protections remains hollow for those who are effectively excluded from the digital ecosystem. Scholars such as Van der Spuy have advocated for treating access to the internet and digital services as a fundamental human right, especially in developing regions where digital access often determines an individual's ability to participate in the modern economy.[39] As such, a data protection framework for Africa should explicitly mandate that governments work toward universal digital inclusion as a core part of their legal obligations.

---

[34] Milan, Stefania, and Emiliano Treré. "The Rise of the Data Poor: Digital Sovereignty and the Inequality of Data Protection." Big Data & Society, 2020.

[35] Boshe, P., Hennemann, M., & Meding, R. (2022). African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward. Global Privacy Law Review.

[36] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010).

[37] Karen Eltis, *Courts, Privacy and Data Protection in the Digital Environment* (Springer, 2019).

[38] Sutherland, E. (2018). Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance.

[39] Titi Van der Spuy, "Internet Rights in the Global South: How the Digital Divide Impacts the Fight for Rights," *Global Media Journal* 15, no. 29 (2019): 43–58.

In addition to addressing digital inclusion, African data protection laws must also accommodate local governance structures and legal traditions. This is particularly important given the diversity of governance models across the continent, from centralised systems to decentralised and traditional authorities. For instance, countries with strong local governance structures may benefit from decentralised data protection oversight bodies, which could ensure that local realities inform data protection practices.[40] Scholars have long pointed out that a one-size-fits-all approach in applying European models can be counterproductive in Africa, where legal and political traditions vary significantly between regions.[41] Therefore, African data protection frameworks should be flexible enough to incorporate different governance structures while still maintaining overarching principles of privacy and data security.

Another key pillar of an effective framework would be technological adaptability. African nations, particularly those with limited digital infrastructure, face rapidly changing technological environments, which can render static legislation obsolete. As demonstrated by the rapid rise of mobile money systems in East Africa, technological innovation often outpaces legislative responses,[42] a robust data protection framework should therefore be adaptable, allowing it to evolve with emerging technologies like artificial intelligence, big data, and the Internet of Things. This can be achieved by building flexibility into the legal framework, allowing regulatory bodies to issue guidelines and updates in response to technological developments, rather than relying solely on statutory amendments, which can be slow and politically fraught.

The proposed framework must also tackle the challenge of data sovereignty. In an increasingly globalised digital economy, African countries face the challenge of managing cross-border data flows while retaining control over their own data.[43] The European GDPR's principle of data localization—where data is stored and processed within the region's borders—offers one potential model, but its wholesale application in Africa may be problematic.[44] African countries, with their varying capacities for data storage and processing, may not be in a position to implement such policies without significant economic costs.[45] A more practical solution would be for African data protection laws to focus on ensuring that foreign companies handling African data are subject to African legal standards, similar to how the GDPR applies to non-EU companies processing European data. This

[40] Alexander B. Makulilo, "Privacy and Data Protection in Africa: A State of the Art," International Data Privacy Law 2, no. 3 (2012): 163–178.

[41] Makane Moïse Mbengue, "Decentralizing Data Protection: African Lessons for the Global South," *African Journal of International Law* 20, no. 3 (2021): 128–144.

[42] Susan Johnson, "The Emergence of Mobile Money in East Africa: Financial Inclusion or Exclusion?" World Development 48 (2013): 82–95.

[43] Susan Ariel Aaronson, "Data Is Different: Why the World Needs a New Approach to Cross-Border Data Flows," *International Affairs* 96, no. 3 (2020): 767–789.

[44] Kuner, C. (2023). Protecting EU data outside EU borders under the GDPR. Common Market Law Review.

[45] Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26.

would assert African control over its data while allowing for the continued benefits of cross-border data processing and cloud services.[46]

The *African Union's Convention on Cyber Security and Personal Data Protection* offers a potential starting point for the development of a pan-African framework that addresses these various issues. However, it remains limited in scope and under-implemented.[47]One of its critical shortcomings is its failure to emphasise the link between data protection and digital inclusion, as well as its relative silence on the question of data sovereignty. For this reason, an updated and more robust African framework must build on the AU's Convention by emphasising both the need for digital infrastructure development and the regulation of foreign data processors who operate on the continent.[48]

A final component of this framework should be a strong enforcement mechanism. One of the greatest challenges facing the implementation of data protection laws in Africa is the lack of institutional capacity to monitor and enforce compliance.[49] Countries like South Africa and Kenya, which have introduced progressive data protection laws, still struggle with the practical realities of enforcement due to limited resources and technical expertise.[50] Therefore, an African framework must prioritise capacity building, both in terms of technical expertise and regulatory infrastructure. This could involve regional cooperation, where countries pool resources and expertise, as well as partnerships with international organisations that can offer technical assistance. Without robust enforcement mechanisms, even the most progressive legal frameworks risk becoming ineffective.[51]

8. Conclusion

The digital divide in Africa is not merely a technological gap; It is a pressing socio-economic issue that challenges the effective implementation of privacy and data protection laws in the context of the Fourth Industrial Revolution. As illustrated through the experiences of individuals like *Mama Marriam*, legislative frameworks must account for the realities of digital exclusion to be truly effective. Policymakers must prioritise inclusive approaches that bridge the digital divide, and ensure that privacy protections extend to all citizens, regardless of their technological access. A forward-thinking, equitable legislative environment has the potential of empowering marginalised communities while safeguarding their digital rights which would contribute to a more just and inclusive digital economy.

---

[46] Anupam Chander, *The Electronic Silk Road: How Data Flows Are Shaping the Global Economy* (Stanford: Stanford University Press, 2013).

[47] Mohamed Aly Bouke, Sameer Hamoud Alshatebi, Azizol Abdullah, Korhan Cengiz and Hayate El Atigh. "African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions." ArXiv, abs/2307.01966 (2023).

[48] African Union, *Convention on Cyber Security and Personal Data Protection* (2014).

[49]Mohamed Aly Bouke, Sameer Hamoud Alshatebi, Azizol Abdullah, Korhan Cengiz and Hayate El Atigh. "African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions.

[50] Thulani Madondo, "The Challenges of Enforcing Data Protection in Africa: A South African Perspective," *Information & Communications Technology Law* 29, no. 4 (2020): 327–345

[51] S. Hamid and R. Mihet. "Big Data, Internet Privacy and the Vulnerabilities of the African Regulatory Landscape." European Journal of Business and Management (2020).

REFERENCES

Books

1. Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business and Society*. Oxford University Press, 2002.
2. Chander, Anupam. *The Electronic Silk Road: How Data Flows Are Shaping the Global Economy*. Stanford University Press, 2013.
3. Dijk, Jan van. *The Network Society: Social Aspects of New Media*, 2nd ed. Sage Publications, 2006.
4. Eltis, Karen. *Courts, Privacy and Data Protection in the Digital Environment*. Springer, 2019.
5. Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.
6. Norris, Pippa. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press, 2001.

Journal Articles

1. Aaronson, Susan Ariel. "Data Is Different: Why the World Needs a New Approach to Cross-Border Data Flows." *International Affairs* 96, no. 3 (2020): 767–789.
2. Antonova, Slavka, and Ernest J. Wilson. "St Antony's International Review." 3, no. 1 (2007): 99–101.
3. Boshe, P., M. Hennemann, and R. Meding. "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward." *Global Privacy Law Review*, 2022.
4. Bukht, Rumana, and Richard Heeks. "Digital Economy Policy in Developing Countries." *Economics of Innovation and New Technology* 23 (2014): 802-824.
5. Evangelista, R., P. Guerrieri, and V. Meliciani. "The Economic Impact of Digital Technologies in Europe." *Economics of Innovation and New Technology* 23 (2014): 802-824.
6. Fuchs, Christian. "Towards a Critical Theory of Cyberspace." *Journal of Information, Communication and Ethics in Society* 2 (2005): 64–68.
7. Greenleaf, G., and B. Cottier. "Comparing African Data Privacy Laws: International, African and Regional Commitments." *International Data Privacy Law* 3 (2013): 42–50.
8. Hamid, S., and R. Mihet. "Big Data, Internet Privacy and the Vulnerabilities of the African Regulatory Landscape." *European Journal of Business and Management* (2020).
9. Hollman, A., T. Obermier, P. Burger, and A. Spanier. "Rural Measures: A Quantitative Study of the Rural Digital Divide." *Journal of Information Policy* (2020).
10. Kuner, C. "Protecting EU Data Outside EU Borders Under the GDPR." *Common Market Law Review* (2023).
11. Lawrence-Ogbeide, Efe, Chiemeka Felix Nwosu, and Olumide Babalola. "A Value Assessment of Personal Data: Towards Greater Privacy Consciousness in Africa." *International Journal of Law and Society* (2023).

12. Madondo, Thulani. "The Challenges of Enforcing Data Protection in Africa: A South African Perspective." *Information & Communications Technology Law* 29, no. 4 (2020): 327–345.
13. Milan, Stefania, and Emiliano Treré. "The Rise of the Data Poor: Digital Sovereignty and the Inequality of Data Protection." *Big Data & Society*, 2020.
14. Makulilo, Alex B. "Data Protection Regimes in Africa: too far from the European 'adequacy' standard?" *International Data Privacy Law*, 3 (2013): 42-50.
15. Sutherland, E. "Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance." *The Journal of African Law* 64, no. 2 (2020): 245-267.
16. Van der Spuy, Titi. "Internet Rights in the Global South: How the Digital Divide Impacts the Fight for Rights." *Global Media Journal* 15, no. 29 (2019): 43–58.

Reports

1. International Telecommunication Union (ITU). *Measuring Digital Development: Facts and Figures*, 2021. Geneva: ITU, 2021. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf.
2. International Telecommunication Union (ITU). *Measuring Digital Development: Facts and Figures*, 2022. Geneva: ITU, 2022. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2022.pdf.
3. United Nations. *Human Development Report*. New York: UN, 2020.
4. GSMA. *The Mobile Gender Gap Report*. London: GSMA, 2020.

Conventions & Regulations

1. African Union. *African Charter on Human and Peoples' Rights*, art. 5, art. 9.
2. African Union. *Malabo Convention on Cyber Security and Personal Data Protection*, adopted June 27, 2014.
3. Council of Europe. *Resolution (73) 22 on the Protection of the Privacy of Individuals with Regard to Automatic Processing of Personal Data*, 26 January 1973.
4. European Parliament and Council of the European Union. *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*, 27 April 2016.

Conference Papers and Theses:

1. Bouke, Mohamed Aly, Sameer Hamoud Alshatebi, Azizol Abdullah, Korhan Cengiz, and Hayate El Atigh. "African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions." *ArXiv* abs/2307.01966 (2023).

Other:

1. Ted Turner, as quoted in *The UN World Economic and Social Survey* (2005) 84.