Chapter 10

Responsible data in public services digitalisation in Africa

Jerusha Govender & Diana Zhou

Abstract

Emerging technologies offer unprecedented opportunities for enhancing efficiency in public service processes. However, these advancements may pose risks if they do not pay adequate attention to data ethics and responsible practices, particularly to vulnerable groups. Responsible data practices are imperative for empowering individuals and safeguarding against potential harm from data misuse. This chapter presents a framework for responsible data, highlighting three layers aimed at realising ethical data use within public service digitalisation initiatives. Through analysis of eight cases, ranging from data lifecycle management to governance strategies, key trends emerge: a shift towards responsible data sharing, evolving perspectives on power dynamics, heightened concerns for data privacy, and development of context-specific legal frameworks. Recommendations include tailored guidelines for digital solutions, minimum standards for public participation, and empowerment of communities and data providers. Governance efforts must assess the impact of global initiatives while accommodating diverse African contexts and capacities. This chapter serves as a critical resource for policymakers and implementers, facilitating the enhancement of data initiatives within evolving digital governance frameworks.

Keywords: Responsible data; data governance; public services; digitalisation, data lifecycle, responsible data management, ethics

Introduction

Data-driven technology such as artificial intelligence (AI) and machine learning (ML) offers significant potential for enhancing public services and achieving developmental goals (Hinkley, 2023; Kumar, 2014; Nzimakwe & Pillay, 2010). Technology can increase the impact and reduce the cost of achieving the sustainable development goals (SDGs), enabling a cumulative saving of as much as US$ 55 trillion by 2030 (Force for Good, 2023).

The projected cost-saving value may be overly optimistic, while the pace at which these technologies are advancing poses risks to the users of technology and communities affected,

especially where the underlying considerations for data risks have not yet been addressed (Lolich & Timonen, 2022; Sajevu, 2005). It is unclear to what extent data from citizens is being accessed and used, how secure data are, the extent to which data can be breached for malevolent use cases, and how algorithms and technology may negatively influence decision-making and behaviour (Ahmad, Han & Alam, 2023; Joseph, 2018; Pieterse, 2021; Sajevu, 2005). For example, during the COVID-19 pandemic, privacy concerns were raised when some governments tried to implement COVID-19 apps to digitally trace individuals who had been in contact with infected persons. How secure the apps were and how much governments intended to use the information from them has left many questions (Beqiraj et al., 2021). A rapid expansion of state surveillance practices in Egypt, Kenya, Nigeria, Senegal, South Africa and Sudan is evident, causing a significant violation of privacy rights (Roberts et al., 2021). To address emerging concerns around data access and governance, initiatives for open data, personal data protection, research ethics, ethical AI and other related fields became driving forces contributing to responsible data theory and practice in changing digital contexts, in Africa and globally.

This chapter includes a review of literature, cases, and solutions related to responsible data practices in African public services digitalisation[1]. The analysis and discussion are guided by a framework for responsible data that provides a view of the current and future scenarios and their implications for policy and implementation.

The chapter begins by reviewing the African Union (AU) Data Policy Framework as a blueprint for African data governance, clarifying the concepts of responsible data. It delves into the relevance of responsible data to the growing digitalisation of public services in Africa. We critique cases, and pose an imperative for responsible data frameworks and practices as the foundation on which data-driven technology governance is built.

Defining responsible data

The evolution of data in scientific communities, open data, open government, data and information sharing initiatives, social media and digital data collection applications has

[1] Digitalisation refers to developing tech-enabled processes and systems to improve manual systems, whereas digitisation is more narrowly defined as converting and recording data and information on a digital platform.

prompted discussions on how data is handled from an ethical point of view, leading to the term 'responsible data'. The concept of responsible data emerged from nuanced views on ethics[2] in fields of science, technology, human and social research, and monitoring and evaluation (M&E), among others. In addition to the moral principles and values that guide how data is collected and used, responsibility elevates the obligation to act or be accountable for our actions (Bramon & Leslie, 2012; Torelli, 2020).

Responsibility extends beyond the fields mentioned. In programme design and implementation practices, there is a need for ethics and responsibility. For example, seeking consent or participation from a person is an ethical consideration in research. Creating systems to allow for retraction of consent, adapting how consent is sought from different individuals, and holding the data collector (public or private) accountable for this is a responsibility. Responsible data is closely related to data governance (the authority or control over the management of data), where clear policies and structures are required to ensure that data collected and stored is safe and protected from malicious use.

Few publications provide a holistic definition of what responsible data is, but there are complementary descriptions or elements described across fields. Responsible data in humanitarian sectors is described as "the ethical, do-no-harm and duty of care approaches that should be in place when collecting and using data, especially data from or about vulnerable, minoritised or historically marginalised individuals or groups" (CLEAR-AA & MERL Tech, 2021, part 1:v). In practice, data users should proactively assess what data is sensitive and could cause harm or other negative implications if accessed without authorisation. Data users must put in place measures to protect against these implications. Reliefw Web (2021) describes responsible data as "the safe, ethical, and effective management of personal and non-personal data for an operational response, in accordance with established frameworks for personal data protection". Based on this definition, they developed a guidance document that provides practical steps and tools to ensure responsible data management.

[2] Ethics refers to the moral principles that govern human behaviour. This broad principle is extrapolated from research ethics, where research ethics which encompasses norms of conduct and discourse about delineating good or acceptable from bad or unacceptable behaviour in research.

Group privacy, empowerment-based data usage, and risks to decision-making have emerged as other elements to consider in the definition of responsible data. Responsible data aligns with prioritising people's rights to consent, privacy, security, and ownership when using data in social change and advocacy (Rahman, 2018). An important addition to this definition is the inclusion of implementing the values and practices of transparency and openness. Lastly, the principles for digital development include consideration for designing with the user in mind, understanding the existing ecosystem, building for sustainability, and addressing the power dynamics of data (Principles for Digital Development, 2024). When referring to aspects of responsible data, various definitions include the following terms, words, concepts, or definitions:

Figure 1. Summary of key terms and concepts that introduce responsible data practices

The consolidated definition of 'responsible data' can be framed as an ethical and human rights obligation for data and digital users to ensure that the collection and use of data empowers individuals and groups and protects the providers of data or those affected by the data from harm as a result of inappropriate or incorrect use and interpretation of data. Additionally, in African contexts, indigenous values and practices must be considered.

Public services data and digitalisation

Education, electricity, health, housing, safety, transport, water and welfare constitute the government's critical public services. Effective public services depend on data systems supporting local, regional, provincial, county and national decision-making. Digitalisation of public services is expected to improve service delivery, increase efficiency in using state

budgets, increase accountability and progress toward sustainability (Fischer, Heurberger & Heine, 2021; Leão & Canedo, 2018; Lolich & Timonen, 2022). For example, paper-based systems moved to electronic format have increased the speed of data capture and retrieval of tax data; biometric systems have improved medical diagnosis; and analytics have sharpened the prediction of weather patterns and crop risks (Bamberger & York, 2020).

Data usage and digitalisation were accelerated by the COVID-19 pandemic, strengthening the push for statistical and surveillance offices and national M&E systems to drive data systems for improved and rigorous reporting (CLEAR-AA & MERL Tech, 2021). The AU Data Policy Framework supports the notion that data utilisation is a key driver to achieve Agenda 2063 and the SDGs (African Union, 2022).

The E-Government Development Index (EGDI) provides a global view of the public sector's digitalisation level, related to how a country is using information technologies to promote the access and inclusion of its people (UNSDG, 2022). The 2022 data places Africa at the bottom with a score of 0.4050, well below the global average (UNSDG, 2022).

It is anticipated that African countries' digitalisation of public services will continue to expand, yet governments need to catch up. Contrasting views on the success of African digitalisation flag the social justice challenge in public services, potentially increasing digital divides among those who do not opt in or do not have the digital literacy to navigate new systems (Lolich & Timonen, 2022).

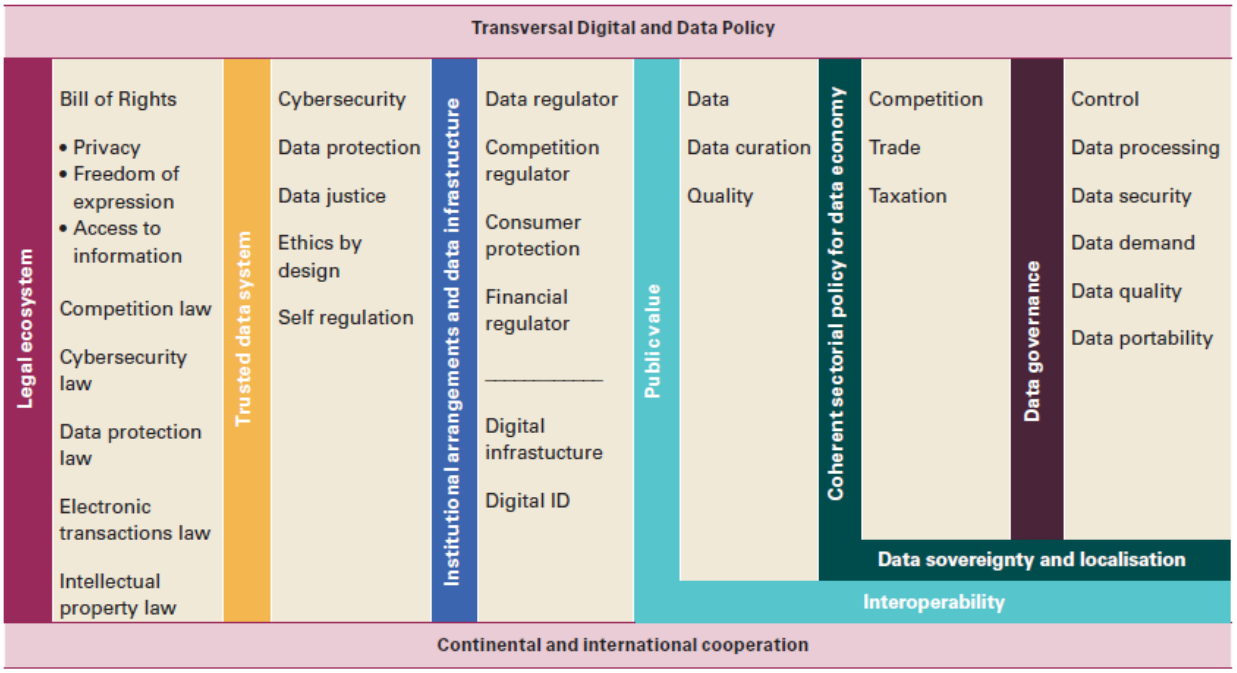
It is a key point in time when responsible data must be addressed within digitalisation frameworks, mitigating the risk of skipping a critical step in solidifying responsible data practices.

A framework for responsible data in practice

Data governance and data management frameworks exist, yet they need to sufficiently address the areas of empowerment and the relationship between practices, people and governance. For example, the commonly used Data Management Body of Knowledge (DMBoK) represents a comprehensive collection of components for data management professionals (The Global Data Management Community, 2024). The AU Data Policy

Framework has become a more prominent guide for strategic data systems in Africa; hence the focus of this section is to provide a blueprint informing a more practical responsible data framework. It includes the components of data governance, data infrastructure, data privacy and protection, data accessibility and openness, and capacity building (Figure 2). The Framework acknowledges that data does not mean the same thing to all communities, and that various other ecosystem factors must be considered in data governance frameworks. Furthermore, the framework makes the role of public-private partnerships as crucial as the roles of other public sector entities (African Union, 2022).

Figure 2. Enabling Data Policy Framework (Source: AU 2022)



The AU Data Policy Framework can be delved into as a reference for responsible data in Africa. It draws from 30 years of attempts to harmonise official statistics in Africa, and has been used as a guide for data protection legislation and cross-border sharing of critical data and information to facilitate trade and development (CIPESA, 2022). Though public sector

data is placed at the core of the framework's focus, one can anticipate its transferability to other sectors, public service entities, and civil society.

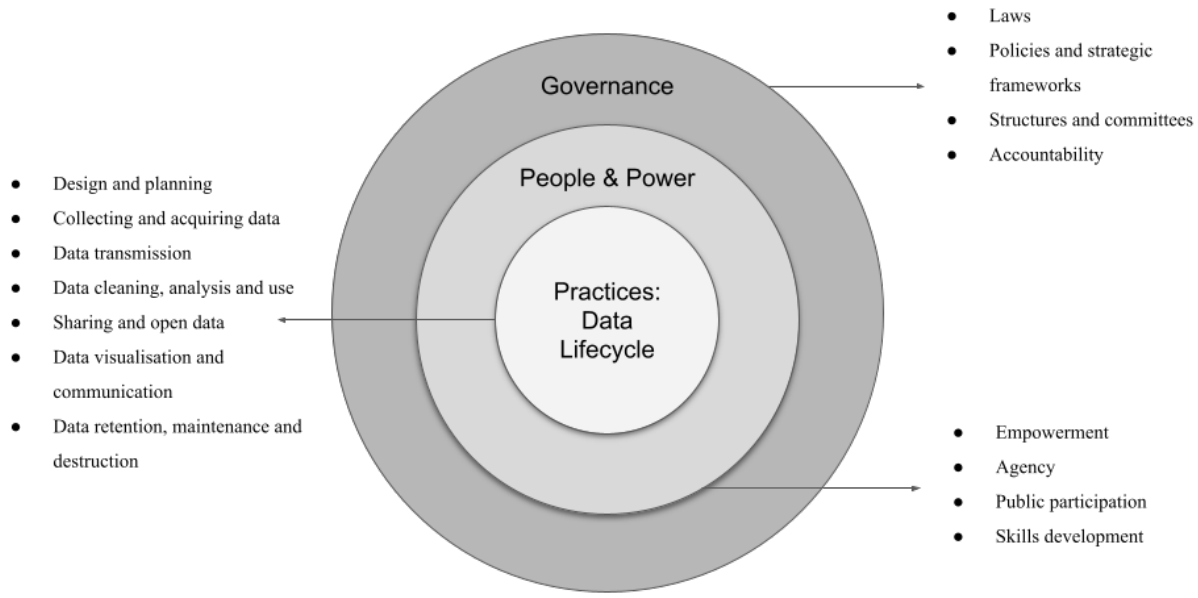
It is argued that the framework does not sufficiently address the demands for further data protection systems at the continental, subcontinental and national levels (Yilma, 2022); it frames a strategic view on how member states may benefit from a data-driven economy, while considering risks and rights. Others have criticised the existing African frameworks or attempts to apply the AU Data Policy Framework to govern data, including for personal data protection, open data and data ownership (Abraham, Schneider & vom Brocke et al., 2019; Pollicy, 2023). The frameworks are fragmented, with competing theories and regulatory domains; a possible reflection of the tension between the social and business value of data.

Though this chapter does not critique the AU Data Policy Framework, it highlights its strategic value, and flags that its implementation is in the hands of regional bodies, national government, sector leaders, and public service entities to develop implementation plans. Implementation frameworks such as DMBoK have yet to catch up to the AU Data Policy Framework, leaving space for a more pragmatic blueprint for responsible data. To this end we propose a responsible data framework from a public services perspective, where focus is placed on the components that support not only the security of data but the overall design, collection, and use of data (Van Ooijen et al., 2023). It is assumed in the framework that data is digitally and non-digitally enabled and is informed by an aim to optimise public access to services and social justice.

We propose a consolidated responsible data framework constituting practices, people-centric approaches, and governance, summarised in Figure 3. The three layers of the framework provide the structure and elements for realising responsible data in public service digitalisation. The layered structure identifies the independent, non-sequential areas and differentiates between the core and the overarching nature of the domains. Practices are placed at the core, as the starting point for designing and implementing responsible data practices. The second layer represents people and power considerations that encapsulate why and how practices are adapted to fit the varied contexts. The outer layer addresses all data and digital governance requirements that are specific to a community or country context. The

following subsections further describe the layers' alignment points with the AU Data Policy Framework.

Figure 3. Framework for responsible data in public services



Practices

Responsible data practices laid out in a lifecycle view can be applied to multiple data collection or extraction practices. A data lifecycle view is appropriate and critical as "responsibility concerns, and important decision points, arise in data sharing, annotation, acquisition, curation, cleaning, and integration" (Stoyanovich et al., 2022:69). Decision-making must be anchored in upholding the rights of people and doing so in an ethical manner. The lifecycle view proposes a sequential set of actions from design to destruction. Government, civil society, academia and industry initiatives around data responsibility, whether through the issuance of guidelines, practice notes or training packs, etc., define the data lifecycle with the same standard components (Global Fund to End Modern Day Slavery, 2020; Oxfam, 2017). The AU Data Policy Framework refers to data security throughout the

data lifecycle, including policies, norms, regulations, legislation and practices to protect data confidentiality, integrity and availability from unauthorised access, corruption or theft. These aspects focus significantly on cyber security and cybercrime (The African Union, (AU) (2022) Data Policy Framework ,2022).

Responsible data practices encompass seven stages:

- Design and planning – requirements for digitalisation are outlined and the context critiqued.
- Collecting and acquiring data – sourcing data for its intended purpose while ensuring the safeguarding of the individuals or groups.
- Responsible data transmission – restricts any loss or theft of private data.
- Responsible data cleaning, analysis and use – accurate hypothesis testing, aggregation and interpretation while limiting the identifiability of individuals and groups.
- Safe and responsible data sharing and open data – transparency and further analysis without affecting future risks.
- Responsible data visualisation and communication – informed and correct interpretation of data and for decision-making.
- Responsible data retention, maintenance and destruction – maintaining the security of the data set.

The guidance for responsible data throughout the data lifecycle provides more practical considerations for trusted data systems, and data systems for control, processing, security and quality as presented in the AU framework (Figure 2). Furthermore, these aspects should be employed in public service implementation plans for digitalisation.

People & power

The Data Values Project (2022a) white paper highights that the inequities entrenched in data concentrate power and often benefit a small group of decision-makers The white paper emphasises that "[w]ithout addressing the ways that data can exacerbate or alleviate inequalities, the push for digital transformation risks reproducing unjust analogue systems" (The Data Values Project, 2022a, section 1.2). Beyond the practical considerations for responsible data are calls for deeper systemic shifts and viewing responsible data from an empowerment lens. The African Union (AU) (2022) Data Policy Framework (2022) elaborates on the need for decentralisation of data and categorisation at levels enabling

understanding of different groups, and policies that support these and other means to shift the asymmetries in power. Furthermore, the AU advocates for ethical control that considers gender roles in African contexts and the creation of enforcement powers at regional and national levels. CLEAR-AA & MERL Tech (2021) introduced consideration for broader user groups of data, accounting for data literacy levels and cultural factors in how information is transferred back to communities or groups from which they were retrieved during design. The Data Values Project (2022b) manifesto highlighted responsible data that serves all and requires political, social, and technical action. The manifesto proposed five actions:

- Empowering people to shape how they are represented in data
- Investing in public participation in the development of data and digital solutions
- Democratising data skills to support local use and engagement in data
- Strengthening cultures of data use and re-use
- Funding open and responsive data systems.

The actions go deeper into the elements that support public value than those presented in the AU framework (Figure 2), humanising data value and curation. These actions may be reframed as the principles that must underscore digital transformation and digitalisation strategies.

Governance

Responsible data practices must be led by the acts, policies, and laws that govern data issues, from privacy to ethical use of data. Good governance is constituted by the core principles of transparency, accountability, participation, and the rule of law (De la Harpe et al., 2008). Among other definitions, the main ingredients are legal systems and structures that enforce responsible data governance and create channels for fair action and recourse. The AU articulates the need for data governance standards, rules, norms and principles to address data risks while enabling data economy development. Data privacy acts, data strategies, and ministerial data governance committees are practical ways to establish responsible data governance. CLEAR-AA & MERL Tech (2021) state that "[b]eyond data management, data privacy, and data protection, data governance includes the end-to-end policies, strategies, standards, rights and accountabilities for the data". Governance holds the most significance in the framework, as it creates the boundaries for accountability and addressing responsible data. The four key components of governance are:

- Laws that address ethical and responsible data across sectors and are regulated and enforced by governments
- Policies and strategic frameworks that guide national focus on responsible data and integrate with digital and information policies
- Structures and committees that are tasked with regulating and supporting the implementation of policies and frameworks
- Accountability channels that ensure responsible data offenders are reprimanded and that there are lines of communication to report deviance.

The data governance components are closely aligned with the elements of a legal ecosystem, data economy, and data governance in the AU framework (Figure 2). We emphasise the overarching nature of data governance that must be considered in digitisation policy and strategy, while positioning practice, people and power at the core of public service digitalisation.

Methodology

A qualitative case study approach was taken to assess the emerging trends in responsible data in practice. Case studies allow for in-depth investigation of complex and contemporary issues and provide real-life context (Crowe et al., 2011). This approach was selected due to the emergent state of responsible data and a focus on evidence of application. Though there are many applications of data privacy, security and governance, the broader concept of responsible data in public service digitalisation is yet to be fully realised.

Cases were selected using typical and diverse methods (Seawright & Gerring, 2008). Eight cases were identified, and four were chosen for demonstrating responsible data practices across various stages of the data lifecycle, measures to shift power in data ecosystems, and national governance practices. The selection criteria included demonstrating elements of the responsible data framework (Figure 3), relevance to public services in Africa, sufficient publicly available data for analysis, and implementation between 2000 and 2024. Data were collected through document analysis and interviews with five key informants to validate and supplement the information.

The cases were thematically analysed using the responsible data framework. Each layer and element of the framework in each case was assessed and assigned a weight from zero to

three: three if all elements within a layer were evident, two if some elements were evident, one if at least one element was described but not implemented, and zero if no elements were addressed. Comparisons were made across cases, framework layers and elements.

Analysis: Responsible data in practice

South Africa, alongside Botswana, Kenya, Rwanda, Nigeria, Uganda, Togo and Ghana, is a 'front-runner' in data protection policies and responsible data use (Culture Custodian, 2023; The Citizen Tanzania, 2023). This section is a deep dive into analysing the selected cases, presented as case reports. The cases are mainly from South Africa, a country considered to be leading in African data governance, in addition to two cases from Uganda and a global initiative.

The analysis shows that all cases demonstrate consideration for at least one layer of the responsible data framework (practice (data value chain), people and power, governance) (Table 1), with varying levels of implementation. Although we did not assess the quality of implementation, the evidence indicates that the application of practices aligned with the data lifecycle is prevalent in all cases, but varies. Further inspection reveals that the case of Ugandan refugees, where data issues are closely tied to people's daily activities, shows the most substantial demonstration of data practices aligned to the data lifecycle.

In contrast, governance is significantly considered only in government and global initiatives, with little evidence of adapting governance for national or smaller projects. This observation might reflect the role of governments in establishing regulations and policies that align with the global community.

The layer concerning people, particularly in terms of power, is emerging as a central aspect that needs more explicit guidelines and depth in implementation, especially in the public sector (e.g. gun detection and data strategies cases). On the other hand, the case study from the humanitarian sector provided some examples concerning people and power. As discussed in the earlier section, responsibility issues appear to be led by the humanitarian sector, which is committed to upholding human rights as one of its core responsibilities, making the people aspect evident in this context.

Table 1: Summary of key characteristics of selected responsible data cases

Case	Period	Location	Responsible data framework layer*		
			Practices	People & power	Governance
1.Data strategies at multi-levels	2013-2024	South Africa	✓	-	✓✓✓
2. e-Government systems in public service	2012-2024	South Africa	✓✓	✓	✓
3. UNU WIDER open data initiatives	2014-2024	South Africa; Uganda	✓✓	✓	✓✓
4. Gunshot detection solution deployed in the City of Cape Town	2016-2025	South Africa	✓✓	✓	✓
5. Stock Visibility Solution implementation evaluation	2014-2017	South Africa	✓✓	✓	✓
6. Responsible Data for Children data lifecycle	2019-2020	Uganda	✓✓✓	✓✓	✓
7. Lacuna Fund addressing bias in ML datasets	2020-2023	Kenya; Multiple	✓✓	✓✓	✓
8. Leave No One Behind global initiative	2019-2022	Multiple	✓	✓✓	✓✓✓

***✓✓✓** *Multiple examples and all elements addressed within layer evident in the case;* **✓✓** *Some examples of at least one element within layer evident in the case;* **✓** *At least one element described within layer with no examples implemented in the case; – No evidence of any element of the layer addressed in the case*

The following case reports describe four of the cases in detail, unpacking the overall emerging insights in line with the responsible data framework.

Case 1: South Africa's data security strategies

In the section on AU Data Policy presented earlier in the chapter, the development and implementation of data protection laws are crucial for responsible data management, particularly in African countries undergoing digital transformations in public services such as healthcare, economy, etc. (African Union, 2022).

Privacy and data protection in South Africa are comprehensive and multi-faceted, involving constitutional protections, data protection laws, surveillance practices, and sector-specific policies. For instance, the Protection of Personal Information Act (POPIA), enacted in 2013, governs data protection and established the Information Regulator responsible for overseeing compliance (South African Government, 2023b; Information Regulator, 2020). Data subjects in South Africa have several rights under POPIA, including the right to access their data, request correction or deletion, and object to processing. POPIA has adopted a conditional flow of data, which some consider a balanced approach, to align with international human rights standards and avoid strict data localisation measures (Atuguba Akongburo et al.,, Boshe & Hennemann 2024). This includes ensuring recipient jurisdictions guarantee international human rights standards.

Real-life examples (chosen only for the purpose of illustrating the POPIA act) illustrate the complexities of balancing privacy and information access under POPIA (Pinto et al., 2024; Britton, 2022). One notable case involves the Landmark Foundation Trust, which requested digital records on leopard-related permits in the Eastern Cape from 2017 to 2019 (SAFLII, 2022). The request was denied, avoiding unreasonable disclosure of personal information. The court had to balance privacy rights with access to information under PAIA and POPIA, emphasising that not all personal information is protected from disclosure. The decision depended on whether disclosure would be unreasonable, considering transparency, public interest, and sufficient evidence for refusal.

Another example is the South African Matric exam, for which previously the Department of Education had publicly published the results. In 2022, the Information Regulator instructed

the Department to seek the consent of the learners or their parents. Adams & Burger-Smidt (2022) posited that a "[r]obust understanding of what consent actually requires and when it should be obtained is without doubt important".

Exemptions under POPIA are allowed in certain cases, but compliance remains paramount (Burger, 2023). The Information Regulator has received numerous complaints related to alleged POPIA violations, indicating the importance of compliance and assessment (Malinga, 2023).

South Africa's legislative framework aims to regulate the entire data value chain, yet obstacles persist in the finalisation of policies, effective implementation, oversight, and balancing rights with security and development objectives. The absence of national data governance policies exacerbates these challenges, leading to sector-specific initiatives such as the City of Cape Town's draft data strategy (City of Cape Town, 2023b). Delays in finalising the Draft National Data and Cloud Policy – finally signed by the Minister of Communications and Digital Technologies on 27 March 2024 (South African Government, 2024) – left a vacuum in policy direction, which raised concerns, particularly regarding skills and knowledge gaps (South African Government, 2023a; De Wet, 2023). The National Data and Cloud Policy (NDCP) aims to strengthen state capacity for service delivery and policy development based on data analytics, and to promote data sovereignty and security (South African Government, 2024). The policy includes strict data localisation requirements for critical information infrastructure and data generated from natural resources, mandating that such data be processed and stored within South Africa. In addition, it aims to create an enabling environment for data and cloud services to support socio-economic development, promote connectivity, remove regulatory barriers, and ensure cybersecurity and privacy.

Some argue that South Africa's emphasis on data sovereignty and localisation could potentially conflict with the need for global data integration and cooperation, especially in sectors that rely on international data flows for innovation and economic growth (Atuguba Akongburo et al., 2024).

The proposed framework in this chapter advocates for a proactive and prescriptive approach regarding responsible data. The POPIA, for example, needs to be more prescriptive, especially in aspects of data handling. The framework ensures accountability and security, requires lawful data collection, consent-based data sharing, adequate protection, and secure disposal of personal data, ensuring it is not kept longer than necessary and is securely disposed of. However, the POPIA must include directions on what actions to take by the responsible party (the guilty party) to mitigate damage, the degree of responsibility and cooperation with the Information Regulator, and the effectiveness of administrative fines (Lee, 2022).

Case 2: e-Government projects in the South African government

The South African National Development Plan 2030 articulates the vision for the country (National Planning Commission, 2012). The country is still grappling with the triple challenges of poverty, unemployment and inequality, which the COVID-19 pandemic compounded. For years, the government has implemented various digital data systems to digitise government services to improve governance, efficiency and service delivery. There have been notable successes, challenges and lessons learned in implementing such systems.

The National Population Register (NPR), developed by the South African Department of Home Affairs, provides a database with records of citizens' significant life events from birth to death to facilitate service delivery and good governance (Parliamentary Monitoring Group, 2023). The system requires high levels of security in how data is collected, stored and shared responsibly. Data protection laws then become critical; and as discussed in the previous section, such acts include PAIA and POPIA, among others. Quality issues have been raised regarding the completeness of the NPR, for various reasons, e.g. late birth registrations, incomplete information, and fraud cases (e.g. fake marriages). To mitigate these issues, the department has embarked on various campaigns, including a campaign encouraging early birth registrations (Parliamentary Monitoring Group, 2023).

In 2010, a campaign was launched to encourage new births to be registered within 30 days, and citizens were entitled to receive identity documents on turning 16 (South African Government, 2010). These efforts were part of a broader strategy to maintain a secure and credible NPR, which is crucial for accessing rights, benefits and opportunities in both the

public and the private sector. However, the department has faced criticism of the 30-day rule. In 2023, a case was brought to the courts by the South African human rights organisation the Legal Resources Centre (LRC) regarding the cumbersome process to register children whose parents live in remote areas and who are from low-income households, which makes it difficult to travel and register the births (Macdonald, 2023). Systems should be inclusive, aligned with the Constitution. and not leave any part of society at a disadvantage or excluded.

The Department of Home Affairs integrated its systems with other departments (e.g. Education) and some private firms such as banks, by means of which certain services are offered, such as issuing of identity documents. The Department recently drafted the National Identification and Registration Bill, 2022, to establish a single, inclusive and integrated national identification system for the Republic, among other provisions (Parliamentary Monitoring Group, 2023). Having such sensitive and personal information about the entire population in one database can attract cyberattacks and compromise the information; hence, such initiatives must consider responsible data elements.

The South African Revenue Service (SARS) introduced eFiling for tax returns. Established by the South African Revenue Service Act 34 of 1997, SARS serves as the country's tax authority. Over the years, the agency has improved its services through innovation and technology, integrating with different data sources, including banks, retirement funds, medical insurance providers and others (South African Government, 2021). The eFiling system has significantly improved tax filing efficiency and compliance, making the process easier and more accessible for taxpayers. SARS understands that while the eFiling system leverages technology, a portion of the population requires assistance, so there is a provision to submit returns at SARS branches (SARS, 2023). Connecting to a wide range of databases raises security concerns regarding taxpayer information, so the system must ensure resilience against cyberattacks – which SARS has managed to protect against, as there have been no reported attacks.

Implementing e-government projects involves a complex interplay of technical, social, economic and political factors. The South African government, like many others, is continuously working to balance these interplays to improve its e-government service offerings.

Case 3: Sound detection technology to respond to gang and poaching crime in South Africa

Emerging technology, including drones, biometric systems and AI, is being introduced to improve efficiencies in public services. Much of this remains in test or pilot cases, with pending progress in terms of scale. The novel data sources used or generated by these technologies raise queries around our assumptions about the responsible data principles in these new cases.

One such technology is the ShotSpotter, which SoundThinking describes as "a proven acoustic gunshot detection system that alerts law enforcement to virtually all gunfire within a city's ShotSpotter coverage area within 60 seconds, enabling police to provide a consistent, rapid, and precise response" (SoundThinking, 2024). Reviews have varied regarding the actual benefits of the technology, and there are controversial issues, such as bias regarding the locations where the devices are installed. In the United States, where the technology has been widely used, media articles have highlighted controversies surrounding the technology, pointing out issues such as inaccuracy, racial bias and cost inefficiency (Ebrahimji, 2024; Gwidt, 2024). While ShotSpotter claims accuracy as high as 97%, reports from cities such as Chicago and others reveal a high rate of false positives (Gee, 2022) and of underreporting (Carr, 2021). A Chicago Inspector General report found that only 9% of ShotSpotter alerts led to evidence of a gun-related crime, introducing doubt as to its utility for police departments.

In 2016, SoundThinking (previously ShotSpotter) deployed gunshot detection technology in Hanover Park and Manenberg in Cape Town, South Africa, as a crime prevention initiative (SoundThinking, 2016). The aim of using sound data to address a significant gang-related issue in communities was appropriate, as most of the murders in these communities are gun-related. In 2018, during a Police Oversight, Community Safety and Cultural Affairs meeting, concerns were raised regarding ShotSpotter's effectiveness and potential over-policing in marginalised communities, with suggestions for Cape Town to consider alternative violence-reduction programmes (Parliamentary Monitoring Group, 2023). Various media outlets and interested parties continued weighing in on the efficacy of the technology, and the project was further expanded to Lavender Hill in 2022. Proponents argue the system detects

shootings in real time and improves police response, leading to increased firearm recoveries and reduced incidents. However, community policing forums and residents argue the technology has not achieved its intended impact, with ongoing violence and high costs (GOOD, 2022; Engineering News, 2022; Masson, 2022; City of Cape Town, 2023a; Tech Central, 2023; Duval & Lukas, 2024; Petersen, 2024; Solomons, 2024; Malinga, 2022). In 2022, community members raised concerns about the cost/benefit ratio of this initiative, demanding a need to understand the choices made on behalf of the community and associated costs[3] in a context rife with other inequities.

From a responsible data perspective, these concerns did flag the importance of clear communication around the value and cost of the data collection to address systemic and community issues, as well as community involvement in the deployment of tech-gathering surveillance data. In this case, it was found that the concerns were isolated to two police forums and did not yield reasonable alternative proposals, as reported in an email from Alderman JP Smith, Mayoral Committee Member for Safety and Security (City of Cape Town) on 26 February (Smith, 2024).

Other responsible data considerations included secure storage and management by SoundThinking, integrating the initiative into the Emergency Police Incident Control system, and engagement with Police Services stakeholders and data. The level of direct engagement with communities is not explicitly recorded, but it is an example of the workings between national, provincial and local spheres.

The outcomes of the intervention are emerging as positive. Alderman Smith reported that "60% of all murders in the province are linked to illegal firearms; and both police precincts continued to show a decrease in their murder rate as per the most recent crime stats release, so the value cannot be underestimated." (Smith, 2024). Smith (2024) also confirmed that the project accounted for about 1% of the total budget allocated to technology in the Safety and Security Directorate, and less than 0.02% of the total budget. In addition, whole-of-society

[3] Cost for financial years 2022/23 to 2024/25: ZAR23 883 500, equivalent to USD1 239 876 based on the exchange rate on 28 February 2024.

programmes to address inequities continue to be implemented in these communities, funded by Community Services and Health, Economic Development, and the Mayoral Urban Regeneration Programme, among others. Key lessons relate to improving enforcement in response to gun-related incidents, and the engagement needed with local government and the National Police Agency to increase the initiative's effectiveness.

The SoundThinking technology and surveillance applied for anti-poaching in the Kruger National Park has yielded more positive results (BizCommunity, 2019). In this context, the solution was estimated to increase responsiveness to poaching incidence and arrest, providing a case for data and technology that can address a conservation need. The contrasting cases emphasise that technology deployment in different contexts may have differing responsible data considerations, particularly in design and analysis.

Case 4: Mapping the data lifecycle in Ugandan Mental Health and Psychosocial Support services

Responsible data practices involve engaging with local ,communities and ensuring that data processes are inclusive and respectful of diverse perspectives. Initiatives are emerging to involve citizens in decision-making processes related to data use in public services. Tools for responsible data such as the data lifecycle exist for development entities; such as one developed by the CARE organisation, The Responsible Data Maturity Model (Raftree, 2019). The practices outlined in the data lifecycle are both a guide and a valuable tool to assess and build responsible data in development initiatives.

The Responsible Data for Children (RD4C) initiative, a global collaboration between UNICEF and the Govlab, was launched in November 2019 to highlight and support best practices in data handling for children. It aims to develop practical tools for practitioners and foster a broader discussion on responsible data management to improve children's lives, especially vulnerable children such as refugees and those in war-torn zones (Zahuranec, 2019). They are guided by the RD4C Principles, namely that solutions should be participatory, professionally accountable, people-centric, result in prevention of harms across the data lifecycle, proportional, protective of children's rights, and purpose driven.

Since its launch, the organisation has performed case studies in seven countries. This chapter will only discuss the Ugandan case study, as it aligns with the RD4C Principles. In 2020, the RD4C initiative implemented responsible data practices guided by a data lifecycle process (RD4C, 2022). The process elucidated challenges and opportunities in data governance, emphasising responsible data management and effective use of Mental Health and Psychosocial Support (MHPSS) services data to enhance service provision. The project commenced with mapping the data lifecycle of MHPSS data from refugee children to promote the responsible use of such data.

A reflection of how this project demonstrates aspects of the framework and how each of the aspects are addressed or fulfilled is provided below.

Practice

- Design and Planning: The purpose was clearly articulated by highlighting Uganda's urgent need for MHPSS for over 1.5 million refugees, highlighting the RD4C initiative's efforts to improve data systems. The planning stage of the project involved mapping the data lifecycle and identifying challenges in data management, which was conducted through workshops with key stakeholders.
- Collecting and Acquiring Data: There was recognition that stakeholders involved in the welfare of refugees were varied, and as such, data collection points would vary, and emphasis was placed on the importance of responsible data harmonisation and that the process should be inclusive.
- Responsible Data Transmission: There is mention of the need for, though no clear evidence of actual implementation of, a unified national system for data sharing and common standards, which might address the aspect of restricting any loss or theft of private data.
- Responsible Data Cleaning, Analysis and Use: Data cleaning is one of the challenges the project was trying to address in harmonising data categories and tools across institutions. The proposed strategy was the need for a common taxonomy for MHPSS data. However, the responsible aspect is not coming out clearly, especially on ensuring the identifiability of individuals and groups.
- Safe and Responsible Data Sharing and Open Data: This is one of the areas the project aimed to address in terms of lack of motivation or incentive to share data between various stakeholders, and also the need for common platforms and systems. Emphasis was placed on the importance of community involvement in data system design and of putting

more effort into establishing common standards and frameworks for data governance to improve transparency.

- Responsible Data Visualisation and Communication: Not much detail is provided on this aspect, but emphasis is placed on the importance of translating data into meaningful decisions and sharing insights across organisations involved in the refugee space.
- Responsible Data Retention, Maintenance, and Destruction: There is no detailed information on data retention policies or practices. However, the need for a manual or standard operating procedure for responsible data governance is highlighted. On destruction, there are no specific strategies.

People & Power

- Empowerment: The focus on participatory and people-centric data practices is evident. Engaging adolescent refugee girls in focus groups and incorporating their feedback reflects an effort to empower the community.
- Participation: The project utilised workshops and focus groups, and these are good examples of investing in public participation.
- Data Skills: Training VHTs (Village Health Teams) and other stakeholders on MHPSS standards and data use was considered in the project, emphasising the need to democratise data skills.
- Culture: The culture of data use and re-use was identified through the need for a data catalogue and directory to facilitate this process.
- Funding: This was not explicit in the project, though in general, there is emphasis on the need for collaborative efforts and resource allocation to improve data systems.

Governance

- Governance Structure: The project outlined the involvement of various stakeholders, including government officials, UNICEF, UNHCR, and other partners. It further highlighted the need for a comprehensive data governance framework.
- Policies and Standards: Developing a common taxonomy for MHPSS data and a data governance manual were identified as key action items. The importance of policies and strategic frameworks guiding responsible data practices was emphasised.

This case demonstrates the different aspects of practices, governance, people and power of the framework. Some of the areas are more pronounced, especially regarding the collaborative nature of the project. The quality, following conceptualisation and articulation of the practices, could not be elucidated in order to provide a complete review of whether responsible data was succeeding in practice. However, this example demonstrates a case of providing government services to vulnerable groups while also using a participatory approach to ensure responsible data practices.

Discussion

It is clear that cases of African governments and organisations innovating data and digital solutions do exist to improve public services and contribute to the global data and digital economy. The extent to which responsible data is embedded in the cases is varied. The patterns that have emerged are:

*Practices for smaller-scale application of the **data lifecycle** are evident, with growing focus on areas of responsible data sharing towards improving provision of public services*

In the RD4C case the use of the data lifecycle to improve the process of handling data from refugee children is clearly expressed. The case presented is one of small-scale data collection and digitalisation. In broader literature, there are a growing number of instances of responsible practices, as in the data lifecycle being applied to larger digitalisation of data systems for public services as well (Rahul & Banyal, 2020). Ensuring processes that safeguard the individuals represented by the data, in creation, storage, usability, sharing, archiving and destruction, will continue to add value to digital data solution development. Expanding the data lifecycle approach in emerging technology is likely to normalise responsible data.

Responsible data practices require adjustment as the quality of data used in algorithms continues to raise concerns around bias affecting incorrect public service decisions. The quality of data models to address the black-box concerns in algorithms is a responsible data area that must be more clearly integrated into the responsible data frameworks and in practice. The Lacuna Fund case showcases the specific need for labelling, cleaning and creating new fields to improve existing datasets (Chinyamakobvu, et al., 2023).. The Lacuna Fund and its collaborative funders are a case of an initiative that aims to address the bias in

datasets. It demonstrates the usefulness of involving communities in improving data quality. The South African case of the use of campaigns to improve the quality of birth registration is another example of a more specific practice to address data incompleteness.

Innovating using digital solutions, such as the SoundThinking anti-poaching and gunshot detection application, demonstrates that responsible data collection may also require assessment of new technology in design that may provide better sources of data. Data integration systems developed by SARS in South Africa demonstrate the value and responsible approach to digitalisation of public services data systems – reducing cost and effort for public submissions and responses to queries, therefore benefiting the citizens.

People and power perspectives *are emergent but not yet receiving the attention needed*
Engaging key stakeholders is described as a common approach to ensure public participation in the design of reviews of digital data solutions, and during the collection of data using digital solutions. This was apparent in the RD4C case in Uganda, where the intention was to increase the knowledge of stakeholders on responsible data processes and seek their input into the process changes, and not only from an expert perspective. There is limited insight into the extent and depth of the engagement with these stakeholders across all cases, an area in the responsible data framework that may call for more guidelines and case development. The media reports regarding SoundThinking in the City of Cape Town show us what happens when we do not engage or understand the dynamics of the communities in which digital data solutions are introduced. Though the outcomes appear positive, uninformed community members can derail similar solutions, emphasising the critical step of engagement with the public as part of responsible data.

In the South African birth registration case, data collection systems needed more individual consideration, often imposing high financial and opportunity costs. Encouraging entities to adopt participatory data process mapping could enhance engagement depth. The campaign to boost birth registration exemplifies meaningful engagement and contextual understanding when deploying large data systems. Initiatives such as Leave No One Behind (UNSDG, 2022) promote inclusivity in data systems, recognising diverse categories of people.

As a stark contrast, all cases are devoid of terminology referencing (or derivatives of) power, power dynamics, shifting power, or empowerment. The concept as described in the framework is meant to support ownership and public agency to drive influence, and the shared value generated from data. Data trusts, data skills development, open data and data sharing are some initiatives that may support power shifts as part of responsible data. However, more in-depth investigation and use-case development is needed in this area.

Governance *is dominated by data privacy and catalysed by global governance initiatives*
Global funded initiatives are observed as common drivers of data governance initiatives. The World Data Centre was considered a pioneering Open Data initiative in the 1950s (Korsmo, 2010), supporting data access and retrieval in the data lifecycle. UNICEF leads RD4C in collaboration with GovLab. The UNU WIDER initiative is yet another globally driven initiative, implemented in South Africa and Uganda. These initiatives have yielded sharing agreements to support data sharing across entity types, and have developed standards and metrics through setting up secure facilities to access tax data at the lowest level.

National government-driven initiatives are also creating positive strides in data governance. In the UK, the Office for National Statistics implemented secure data service using the Five Safes Framework, ensuring safe data usage under the Digital Economy Act 2017. e-Estonia, digitalising Denmark, and e-Government in South Africa, Kenya and other growing digital economies signal similar trends.
The South African cases present multiple policies and frameworks for sharing responsible data and tech in government at national and lower levels. Skills and knowledge to implement the policies and improve on responsible data governance are areas that require attention.

In summary, the key themes that have emerged from the case study analysis are:

- The need for a participatory culture for all stakeholders involved
- The need for clear legislature that is implementable
- Robust acts and policies that fit national and local contexts
- The deepening of an understanding of power in data ecosystems and implications for responsible data.

These emerging patterns and themes reinforce recommendations for public services, policymakers, and digital practitioners to demonstrate and implement responsible data practices. Policymakers should also assess the impact of existing policies, prioritising the needs of vulnerable groups such as women, children and refugees. The broader civic society plays a significant role in promoting responsible data, whether through grassroots efforts or the development of frameworks, tools and initiatives aligned with their ethos and organisational mandates.

Conclusion

The insights in this chapter apply to all data-collecting or -generating technologies, both current and emerging in their application in public services. As digitalisation becomes more widely integrated into data systems in public services, the framework for responsible data will become increasingly relevant, prompting further examination and guidance. It is crucial to shift away from a narrow perspective of data responsibility focused solely on ethics and privacy, and instead consider the mechanisms and practices of responsible data. The case study findings present an opportunity for further research into the extent to which the AU Data Framework and other data and digital frameworks are applied in public services. Additionally, the lessons call for advocating for the enforcement of responsible data practices that prioritise people and power, refine and expand existing practices, and permeate through data governance structures across sectors and entities, including grassroots.

References

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*(-), 424-438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Adams, D., & Burger-Smidt, A. (2022, August 3). *POPIA and consent, the biggest misunderstanding?* Werksmans Attorneys. https://www.werksmans.com/legal-updates-and-opinions/popia-and-consent-the-biggest-misunderstanding/

African Union. (2022, February). *AU data policy framework*. https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

Ahmad, S. F., Han, H., & Alam, M. M. (2023). Impact of artificial intelligence on human loss in decision making, laziness and safety in education. *Humanit Soc Sci Commun, 10*(311). https://doi.org/10.1057/s41599-023-01787-8

Atuguba Akongburo, R., Boshe, P., Dei-Tutu, S. A., & Hennemann, M. (Eds.). (2024). *African data protection laws: Regulation, policy, and practice.* De Gruyter. https://www.degruyter.com/document/doi/10.1515/9783110797909/html?lang=en

Bamberger, M., & York, P. (2020). *Measuring results and impact in the age of big data: The nexus of evaluation, analytics, and digital technology.* The Rockefeller Foundation. https://www.rockefellerfoundation.org/wp-content/uploads/Measuring-results-and-impact-in-the-age-of-big-data-by-York-and-Bamberger-March-2020.pdf

BizCommunity. (2019, September 23). *ShotSpotter technology helps Kruger National Park fight rhino poaching.* Bizcommunity. https://www.bizcommunity.com/Article/196/373/195827.html

Bramon, B., & Leslie, J. (2012). Slavery and human trafficking. In *Encyclopedia of Aapplied Eethics* (Second ed., pp. 114-121). Academic Press. https://doi.org/10.1016/B978-0-12-373932-2.00297-0

Britton, N. (2022, April 1). *POPIA is gradually making its way to South African courts.* Clyde & Co. https://www.clydeco.com/en/insights/2022/03/popia-is-gradually-making-its-way-to-our-courts

Burger, A. (2023, October 4). *Information Regulator grants its first exemptions under POPIA.* Werksmans Attorneys. https://www.werksmans.com/legal-updates-and-opinions/information-regulator-grants-its-first-exemptions-under-popia/

Carr, J. (2021, January). *Measuring the effects of ShotSpotter on gunfire in St Louis County, MO.* Policing Project, NYU School of Law. https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/603923e3a32c3f57d67dabec/1614357476874/Measuring+the+Effects+of+Shotspotter+on+Gunfire+in+St.+Louis+County%2C+MO.pdf

Chinyamakobvu, M., Govender, J., James, U., Leslie, T., Letuka, T., & Ncube, A. (2023). *Lacuna Fund Learning and Evaluation Report.* https://idl-bnc-idrc.dspacedirect.org/bitstreams/1908f6da-ae85-4945-ae92-4860339e9f9a/download

CLEAR-AA & MERL Tech. (2021). *Responsible data governance for monitoring and evaluation in the African context.* MERL Tech. https://merltech.org/guidance-on-responsible-data-governance-the-framework/

CIPESA. (2022, October). *Five takeaways from the 2022 African Union Data Policy Framework.* CIPESA. https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf

The Citizen Tanzania. (2023, February 9). *The state of data privacy and protection in Africa.* The Citizen Tanzania. https://www.thecitizen.co.tz/tanzania/magazines/the-state-of-data-privacy-and-protection-in-africa-4117526

City of Cape Town. (2023a, May 4). *Cape Town using gunshot detection, drones to pinpoint gang violence.* City of Cape Town https://www.capetown.gov.za/Media-and-news/Cape%20Town%20using%20gunshot%20detection,%20drones%20to%20pinpoint%20gang%20violence

City of Cape Town. (2023b, June 20). *Draft data strategy.* UCT Libraries. https://lib.uct.ac.za/government-publications/articles/2023-06-20-city-cape-town-draft-data-strategy

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology, 11*(100), 1-9. http://www.biomedcentral.com/1471-2288/11/100

Culture Custodian. (2023, February 8). *More African countries are taking data privacy and protection seriously.* Culture Custodian. https://culturecustodian.com/more-african-countries-are-taking-data-privacy-and-protection-seriously/

The Data Values Project. (2022a). *The Data Values Manifesto.* Data4SDGs. https://www.data4sdgs.org/sites/default/files/file_uploads/DataValues_Manifesto_EN.pdf

The Data Values Project. (2022b). *Reimagining data and power – A roadmap for putting values at the heart of data.* Data4SDGs. https://www.data4sdgs.org/sites/default/files/2022-07/Final%20White%20Paper%20designed%20%28English%29.pdf

De la Harpe, S., Rijken, C., & Roos, R. (2008). Good governance. *Potchefstroom Electronic Law Journal (PELJ), 11*(2), 2-15. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812008000200002&ln%20g=en&tlng=en

De Wet, E. (2023, June 12). *South Africa working on data and cloud policy.* 4C Group of Companies. https://www.4cit.group/sa-government-working-on-data-and-cloud-policy/

Duval, M., & Lukas, B. (2024, March 13). *It's raining bullets in Nyanga: ShotSpotter shows 589 shots in one weekend.* IOL. https://www.iol.co.za/capeargus/news/its-raining-bullets-in-nyanga-shotspotter-shows-589-shots-in-one-weekend-e80738ee-d62d-421c-8841-02bafcb90fa1

Ebrahimji, A. (2024, February 24). *Critics of ShotSpotter gunfire detection system say it's ineffective, biassed and costly.* CNN. https://edition.cnn.com/2024/02/24/us/shotspotter-cities-choose-not-to-use/index.html

Engineering News. (2022, December 15). *Acoustic gunshot detection project launched in Cape Town.* Creamer Media's Engineering News. https://www.engineeringnews.co.za/article/acoustic-gunshot-detection-project-launched-in-cape-town-2022-12-15

Fischer, C., Heuberger, M., & Heine, M. (2021). The impact of digitalization in the public sector: A systematic literature. *Der Moderne Staat – Zeitschrift für Public Policy, Recht und Management, 14*(1), 3-23. doi/abs/10.3224/dms.v14i1.13

Force for Good. (2023, January). *Technology for a secure, sustainable and superior future: Technology as a force for good, 2023 report.* Force for Good. https://www.forcegood.org/frontend/img/2023-report/pdf/Technology_as_a_Force_for_Good_Report_2023.pdf

Gee, H. (2022). 'Bang!': ShotSpotter gunshot detection technology, predictive policing, and measuring Terry's reach. *University of Michigan Journal of Law Reform, 55*(4), 767.

The Global Data Management Community. (2024). *DAMA DMBOK Images.* DAMA International. https://www.dama.org/cpages/dmbok-images

Global Fund to End Modern Slavery. (2020, March). *Responsible data management guidelines.* Global Fund to End Modern Slavery. https://www.gfems.org/wp-content/uploads/2021/06/RDMGuidance_Mar2020.pdf

Gwidt, D. (2024, March 6). *ShotSpotter leak shows that surveillance tech is used to overpolice black and brown communities.* ACLU of Wisconsin. https://www.aclu-wi.org/en/news/shotspotter-leak-shows-surveillance-tech-used-overpolice-black-and-brown-communities

Hinkley, S. (2023, January 10). *Technology in the public sector and the future of government work.* UC Berkeley Labor Center. https://laborcenter.berkeley.edu/technology-in-the-public-sector-and-the-future-of-government-work/

Information Regulator. (2020, July 01). *Strategic Plan 2022/23 – 2026/27.* Information Regulator (South Africa). https://inforegulator.org.za/wp-content/uploads/2020/07/Strategic-Plan-2022_23-2026-27.pdf

Joseph, R. (2018, Jul/Aug). Data breaches: Public sector perspectives. *IT Professional, 20*(4), 57-64. http://dx.doi.org/10.1109/MITP.2017.265105441

Korsmo, F. L. (2010, February 28). The origins and principles of the World Data Center system. *Data Science Journal, 8,* 11.

Kumar, R. (2014, December 29). *Five ways technology is improving public services.* World Bank Blogs. https://blogs.worldbank.org/governance/five-ways-technology-improving-public-services

Leão, H. A., & Canedo, E. D. (2018). Best practices and methodologies to promote the digitization of public services citizen-driven: A systematic literature review. *Information, 9*(197), 1-19. doi:10.3390/info9080197

Lee, A. W. (2022, October 13). *An analysis of the Protection of Personal Information Act (POPIA) and the European Data Protection Framework* [LLM dissertation, UKZN]. UKZN ResearchSpace. https://researchspace.ukzn.ac.za/server/api/core/bitstreams/b0c76739-2d22-463b-8d2d-ba8c3d8c0ed0/content

Lolich, L., & Timonen, V. (2022). Digitalisation of public services as a challenge to social justice. In M. A. Yerkes & M. Bal (Eds.), *Solidarity and Ssocial Jjustice in Ccontemporary Ssocieties* (pp. 191-200). Palgrave Macmillan. https://link.springer.com/chapter/10.1007/978-3-030-93795-9_18#citeas

Macdonald, A. (2023, March 20). *South Africa's birth registration system challenged over 'unconstitutional' requirements.* BiometricUpdate.com.

https://www.biometricupdate.com/202303/south-africas-birth-registration-system-challenged-over-unconstitutional-requirements

Malinga, S. (2022, December 15). *Cape Town resuscitates controversial crime prevention project.* ITWeb. https://www.itweb.co.za/article/cape-town-resuscitates-controversial-crime-prevention-project/KzQenMjyYGy7Zd2r

Malinga, S. (2023, April 5). *InfoReg resolves 70% of POPIA complaints.* ITWeb. https://www.itweb.co.za/article/inforeg-resolves-70-of-popia-complaints/LPp6VMrByz4MDKQz

Masson, E. (2022, December 14). *ShotSpotter redeployed on Cape Flats, detects 224 shots in first two weeks.* The Mail & Guardian. https://mg.co.za/news/2022-12-14-shotspotter-redeployed-on-cape-flats-detects-224-shots-in-first-two-weeks/

National Planning Commission. (2012). *National Development Plan 2030: Our future – make it work.* South African National Planning Commission. https://www.nationalplanningcommission.org.za/assets/Documents/ndp-2030-our-future-make-it-work.pdf

Nzimakwe, T. I., & Pillay, P. (2010, April). Trends and challenges to enhance service delivery in the public sector. *Administratio Publica, 18*(1), 124-138.

Parliamentary Monitoring Group. (2023). *National Identification and Registration Bill.* Parliamentary Monitoring Group. https://static.pmg.org.za/230418nationalidentificationregistrationbill-4-4.pdf

Petersen, C. (2024, April 3). *Gun Free SA raises alarm after confiscation of pistol modified into fully-automatic firearm.* EWN. https://www.ewn.co.za/2024/04/03/gun-free-sa-raises-alarm-after-confiscation-of-pistol-modified-into-fully-automatic-firearm

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication, 28*(0), 1-21. http://www.scielo.org.za/scielo.php?pid=S2077-72132021000200003&script=sci_arttext

Pinto, T., Sheik, S., & Giles, J. (2024, February 23). *POPIA judgments and cases.* Michalsons. https://www.michalsons.com/blog/tag/popia-judgments

Pollicy. (2023). *State of data governance in Africa* [Blog post]. Medium. https://pollicy.medium.com/state-of-data-governance-in-africa-ad00c75053f6

Principles for Digital Development. (2024). Retrieved from Principles for Digital Development: https://digitalprinciples.org/

Raftree, L. (2019, October 2019). *Responsible data maturity model for development and humanitarian organisations.* ICTworks. https://ictworks.org/wp-content/uploads/2019/11/Responsible_Data_Maturity_Model_10-16-19.pdf

Rahman, Z. (2018). *RD 101: Responsible data principles.* Responsible Data. https://responsibledata.io/2018/01/24/rd-101-responsible-data-principles/

Rahul, K., & Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science, 173,* 364-371. https://doi.org/10.1016/j.procs.2020.06.042.

RD4C (Responsible Data for Children initiative). (2022, September 23). *responsible data for refugee children in Uganda.* Responsible Data for Children. https://files.rd4c.org/RD4C_Uganda.pdf

Reliefweb. (2021, February 3). *IASC Operational Guidance on Data Responsibility in Humanitarian Action.* Relief Web. https://reliefweb.int/report/world/iasc-operational-guidance-data-responsibility-humanitarian-action-february-2021?gad_source=1&gclid=Cj0KCQjw0_WyBhDMARIsAL1Vz8ti--iOblSvmIqRBhv_kBYKbCubzIz5oI0lJNYpPrd1klQL5iEZT1saAmlEEALw_wcB

Roberts, T., Mohamed Ali, A., Farahat, M., Oloyede, R., & Mutung'u, G. (2021). *Surveillance law in Africa: A review of six countries.* Brighton: Institute of Development Studies. DOI: 10.19088/IDS.2021.059

SAFLII. (2022, July 26). *Case no: 1199/2021. South Africa: Eastern Cape High Court, Makhanda.* Southern African Legal Information Institution. https://www.saflii.org/za/cases/ZAECMKHC/2022/42.pdf

Sajevu, M. (2005). *The technological risk and uncertainty in governance and economic development.* European Commission Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/handle/JRC31861

SARS. (2023, July 6). *How to submit an income tax return (ITR12) in respect of individuals.* South African Revenue Service.

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly, 61*(2), 294-308. DOI: 10.1177/1065912907313077

Solomons, L. (2024, May 09). *'It's a bloody joke, to be honest': Scepticism over Cape Town plan to spend R860m on anti-crime tech.* News24. https://www.news24.com/news24/southafrica/news/its-a-bloody-joke-to-be-honest-scepticism-over-cape-town-plan-to-spend-r860m-on-anti-crime-tech-20230509

SoundThinking. (2016, September 29). *Cape Town, South Africa selects ShotSpotter gunfire detection system to help reduce gunfire violence.* SoundThinking. https://www.soundthinking.com/press-releases/cape-town-south-africa-selects-shotspotter-gunfire-detection-system-to-help-reduce-gun-violence/

SoundThinking. (2024, May 9). *Introducing the SafetySmart™ platform.* SoundThinking. https://www.soundthinking.com/safetysmart-platform/

South African Government. (2010, March 23). *Zuma launches SA population registration campaign.* South African Government News Agency. https://www.sanews.gov.za/south-africa/zuma-launches-sa-population-registration-campaign

South African Government. (2021, December 10). *SARS moves to increase and expand the use of data.* South African Government News Agency. https://www.sanews.gov.za/south-africa/sars-moves-increase-and-expand-use-data

South African Government. (2023a, April 13). *Government finalising national data, cloud policy.* South African Government News Agency. https://www.sanews.gov.za/south-africa/government-finalising-national-data-cloud-policy

South African Government. (2023b, November 26). *Protection of Personal Information Act.* South African Government Gazette. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

South African Government. (2024, May 31). *Electronic Communications Act: National Data and Cloud Policy.* South African Government Gazette. https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf

Smith, A. J. P. (2024)., Mayoral, Committee Member for Safety and Security (City of Cape Town) personal(email communication, February 26, 2024).

Stoyanovich, J., Abiteboul, S., Howe, B., Jagadish, H., Schelter, S., Williams, A., Bruderer, H., & Goth, G. (2022, June 1). *Responsible data management.* Communications of the ACM. https://cacm.acm.org/research/responsible-data-management/

Tech Central. (2023, May 05). *Cape Town deploys advanced tech in war on crime.* Tech Central. https://techcentral.co.za/cape-town-deploys-advanced-tech-in-war-on-crime/225290/

Torelli, R. (2020). Sustainability, responsibility and ethics: Different concepts for a single path. *Social Responsibility Journal, 17*(5). ,719-739 https://www.emerald.com/insight/content/doi/10.1108/SRJ-03-2020-0081/full/html

UNSDG. (2022). *Operationalizing leaving no one behind: Good practice note for UN country teams.* United Nations Sustainable Development Group. https://unsdg.un.org/sites/default/files/2022-04/Operationalizing%20LNOB%20-%20final%20with%20Annexes%20090422.pdf

Van Ooijen, C., Ubaldi, B., & Welby, B. (2023). Data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance. In *OECD working papers on public governance, 33.* OECD Library. https://doi.org/10.1787/09ab162c-en.

Yilma, K. (2023). African Union's data policy framework and data protection in Africa. *Journal of Data Protection & Privacy, 5*(3), 1-7. https://ssrn.com/abstract=4253828

Zahuranec, A. J. (2019, November 21). *The GovLab and UNICEF launch Responsible Data for Children (RD4C) initiative.* TheGovLab. https://blog.thegovlab.org/the-govlab-and-unicef-launch-responsible-data-for-children-rd4c-initiative