

Data privacy law in Africa: Emerging perspectives delves into the profound impact of data privacy on individuals, businesses, and governments across the continent. Experts from diverse African nations provide a comprehensive view of the evolving regulatory frameworks guiding data privacy, exploring its legal, social, economic, and cultural implications. Examining emerging contexts such as Artificial Intelligence, vulnerable groups, and the challenges presented by COVID-19, the book sheds light on the present and envisions future trajectories in data governance. A valuable resource for those navigating the intricate intersection of law and technology in Africa, offering innovative solutions and best practices for enhanced data privacy.

Pretoria University Law Press
PULP

www.pulp.up.ac.za

ISBN 978-1-7764485-9-3



9 781776 448593

DATA PRIVACY LAW IN AFRICA: EMERGING PERSPECTIVES

Lukman Adebisi Abdulrauf & Hlengiwe Dube

PULP

DATA PRIVACY LAW IN AFRICA

Emerging perspectives



Editors
Lukman Adebisi Abdulrauf
Hlengiwe Dube

DATA PRIVACY LAW IN AFRICA

Emerging perspectives

Editors
Lukman Adebisi Abdulrauf
Hlengiwe Dube

Pretoria University Law Press

PULP

publishing African scholarship that matters
www.pulp.up.ac.za

2024

Data privacy law in Africa: Emerging perspectives

Published by:

Pretoria University Law Press (PULP)

The Pretoria University Law Press (PULP) is a publisher at the Faculty of Law, University of Pretoria, South Africa. PULP endeavours to publish and make available innovative, high-quality scholarly texts on law in Africa. PULP also publishes a series of collections of legal documents related to public law in Africa, as well as text books from African countries other than South Africa. This book was peer reviewed prior to publication.

For more information on PULP, see www.pulp.up.ac.za

Printed and bound by:

Pinetown Printers, South Africa

To order, contact:

PULP

Faculty of Law

University of Pretoria

South Africa

0002

pulp@up.ac.za

www.pulp.up.ac.za

Cover design:

DN Ikpo

ISBN: 978-1-7764485-9-3

© 2024

TABLE OF CONTENTS

Foreword	v
Contributors	vii
 Introduction	
<i>Lukman Adebisi Abdulrauf and Hlengiwe Dube</i>	
Part I: The status of data privacy in Africa	2
Part II: Data privacy and artificial intelligence	5
Part III: Data privacy and vulnerable groups	6
Part IV: Data privacy during the COVID-19 pandemic	7
Part V: Selected data privacy issues from a comparative perspective	9
 PART I: The status of data privacy in Africa	
 Chapter 1: A quest for an African concept of privacy	
<i>Patricia Boshe</i>	
1 Introduction	13
2 African privacy: Does it really matter?	15
3 Privacy in data protection	21
4 A myth about African privacy	24
5 African privacy: A way forward	27
6 Conclusion	34
 Chapter 2: Data privacy in Africa: Taking stock of its development after two decades	
<i>Alex Boniface Makulilo</i>	
1 Introduction	41
2 The African world view on privacy	45
3 Determinants of privacy concerns in Africa	48
4 Policy and regulatory frameworks for privacy and data protection	60
5 Analysis of data privacy policies in Africa: Patterns and trends	69
6 Conclusion	73
 Chapter 3: An old question in a new domain: Some preliminary insights on balancing the right to privacy and freedom of expression in the digital era under the African human rights law	
<i>Yohannes Eneyew Ayalew</i>	
1 Introduction	79
2 Internet freedom under the African human rights law	84
3 Balancing the right to privacy and freedom of expression: Preliminary insights	92
4 Publication of personal information	95
5 The right to be forgotten	100
6 Conclusion	103

PART II: Data privacy and artificial intelligence

Chapter 4: The ascent of artificial intelligence in Africa: Bridging innovation and data protection

Emmanuel Salami

1	Introduction	112
2	An overview of relevant concepts	115
3	Actual deployments of artificial intelligence in Africa	117
4	How do artificial intelligence systems collect (personal) data?	119
5	Data protection concerns and remedies in the deployment of artificial intelligence in Africa	121
6	Some implications of inadequate data protection law regulations for artificial intelligence systems	134
7	Conclusion	136

Chapter 5: African data protection laws and artificial intelligence – regulation, policy and ways forward

Moritz Hennemann

1	Introduction	141
2	African data protection laws and artificial intelligence: The current state	143
3	A comparative look at the European Union and the GDPR	147
4	Balancing innovation and potential risks: The way forward	148
5	Conclusion	153

PART III: Data privacy and vulnerable groups

Chapter 6: Digital vulnerabilities and the privacy conundrum for children in the digital age: Lessons for Africa

Hlengiwe Dube

1	Introduction	159
2	Digital risks encountered by children in the digital age	163
3	Privacy implications of children's interaction with technology in Africa	170
4	Children's actions that compromise their privacy	182
5	Emerging technologies and processing children's personal information	185
6	Existing frameworks in Africa for children's privacy and child protection online	186
7	Lessons for Africa	191
8	Conclusion and key recommendations	196
9	Conclusion	203

Chapter 7: Gendered digital inequalities: How do we ensure gender transformative law and practice in the age of artificial intelligence in Africa?

Chenai Chair

1	Introduction	207
2	Conceptual framework and approach	209
3	Context	214
4	Gendered harms from AI-based systems	224
5	A gender-responsive policy action and the role of civil society towards privacy and data protection	232
6	Conclusion	234

Chapter 8: Data protection and privacy for social assistance beneficiaries: A South African perspective

Ntando Ncamane

1	Introduction	239
2	Regulation of social assistance	242
3	Regulatory framework to protect data and privacy of beneficiaries	245
4	Challenges	254
5	Recommendations	259
6	Conclusion	263

PART IV: Data privacy during the COVID-19 pandemic

Chapter 9: Tracking COVID-19: What are the implications for data privacy in Africa?

Alex Boniface Makulilo, Rindstone Bilabamu Ezekiel,

Doreen Mwamlangala and Mbiki Msumi

1	Introduction	269
2	COVID-19 contact tracing and modern technology	271
3	Privacy concerns and debates around COVID-19	276
4	COVID-19 and privacy regulation	281
5	Conclusion	288

Chapter 10: Can we trust Big Brother? A critique of data protection measures in South Africa's COVID-19 tracing database

Dusty-Lee Donnelly

1	Introduction	291
2	Government response to COVID-19	293
3	Protection of personal information	298
4	Location monitoring and the public interest exemption	313
5	Future COVID-19 research	315
6	Conclusion	317

PART V: Selected data privacy issues from a comparative perspective

Chapter 11: The regulation of automated decision making and profiling in an era of big data and ambient intelligence: A European and South African perspective

Alon Lev Alkalay

1	Introduction	323
2	Conceptualising and differentiating automated decision making from profiling	326
3	Exploring the extent of regulation under GDPR and POPIA	328
4	Contextualising current regulation in an age of big data and ambient intelligence	347
5	Conclusion	351

Chapter 12: Independence of data protection authorities in Africa: Trends and challenges

Lukman Adebisi Abdulrauf

1	Introduction	355
2	International influence on the conceptualisation of 'independence' of DPAs	357
3	Independence of DPAs in Africa	363
4	Trends and challenges towards 'independence' of DPAs in Africa	371
5	Conclusion	378

FOREWORD

This book, '*Data privacy law in Africa: Emerging perspectives*' emerged at a pivotal moment in the midst of unprecedented global challenges posed by the COVID-19 pandemic. The importance of the right to privacy and data protection became more pronounced globally, particularly in Africa, where the subject matter had not gained significant traction despite two-thirds of African countries adopting data protection laws. Consequently, the spotlight on safeguarding privacy and protecting personal information has significantly increased. Against this backdrop, Africa is also navigating the delicate balance between embracing innovation in the context of digital technologies and tackling the unprecedented challenges associated with the intersection of emerging technologies and law, particularly in privacy and data protection.

The current acceleration of digital adoption, which has prompted society to leverage technology in every facet, has amplified concerns about privacy and data exploitation and prompted the need for robust privacy safeguards and effective data governance mechanisms. Amid the anticipation of favourable consequences stemming from digital transformation, there are profound challenges that confront vulnerable groups such as women and children who find themselves at a much greater risk. The unprecedented data collection mechanisms and the plethora of online platforms have created more privacy challenges, especially in the protection of personal information.

In this book, experts, scholars, and practitioners from various disciplines explore contemporary insights into privacy and data protection from various perspectives. The chapters comprehensively examine the challenges and milestones in privacy and data protection across the African continent. It explores the dynamic nexus between technology, regulatory frameworks, enforcement mechanisms, and the implications on the socio-economic landscape as societies have become data-driven.

From the contributions in the book, it is evident that in Africa, the journey towards effective privacy and data protection governance is still novel and, therefore, necessitates a nuanced understanding of the national frameworks and international best practices. It is also imperative to

balance individual rights with societal needs. This book, which documents the current state of privacy and data protection in Africa, contributes to the ongoing dialogue on the intersection between technology and society, including the obligations of states, individuals, and other stakeholders such as business entities in shaping data governance.

As highlighted in the book, Africa's context presents diverse socio-economic and political realities that usher pronounced challenges and opportunities for privacy and data protection. I hope that the comprehensive insights, analyses, and reflections explored in this book serve as an invaluable resource for policymakers, legal professionals, scholars, advocates, students, and anyone with an interest in the subject of privacy and data protection in the African context.

I am also optimistic that this book is poised to ignite sustained and informed dialogues that will contribute to shaping transformative progress in Africa's evolving digital ecosystem, including the data governance landscape that seeks to address the tapestry of privacy concerns that have become more pronounced.

Pansy Tlakula

Chairperson: Information Regulator, South Africa

CONTRIBUTORS

Lukman Adebisi Abdulrauf

Associate Professor, Department of Public Law, Faculty of Law, University of Ilorin, Nigeria; Fellow, Institute for International and Comparative Law in Africa (ICLA), University of Pretoria, South Africa.

Alon Lev Alkalay

Privacy Counsel (Africa and International Markets), Bolt; Attorney of the High Court of South Africa; Certified Information Privacy Professional (CIPP/E)

Yohannes Eneyew Ayalew

Teaching Associate, Faculty of Law, Monash University, Australia; Lecturer, School of Law, Bahir Dar University, Ethiopia

Patricia Boshe

Senior Researcher at the Research Centre for Law and Digitalisation (FREDI), University of Passau, Germany

Chenai Chair

Founder of My data rights/Senior program officer Africa Innovation Mradi at Mozilla Foundation

Dusty-Lee Donnelly

Senior Lecturer, School of Law, University of KwaZulu-Natal, South Africa

Hlengiwe Dube

Programme Manager, Expression, Information and Digital Rights Unit, Centre for Human Rights, University of Pretoria, South Africa

Rindstone Bilabamu Ezekiel

Lecturer and Dean, Faculty of Law, The Open University Tanzania, Tanzania

Moritz Hennemann

Professor, Chair for Private Law, and Information Law, Media Law, and Internet Law, and Director, Institute of Media and Information Law, Law Faculty, University of Freiburg, Germany

Alex Boniface Makulilo

Professor of Law and Technology, The Open University of Tanzania, Tanzania

Mbiki Msumiis

Lecturer and Head of Department of Constitutional and International Law, The Open University of Tanzania, Tanzania

Doreen Mwamlangala

Lecturer and Head of Department of Economic Law, The Open University of Tanzania, Tanzania

Ncamane Ntando

Lecturer, Mercantile Law Department, University of The Free State, South Africa

Emmanuel Salami

Researcher in Information Technology, Data Protection and Intellectual Property Law, Faculty of Law, University of Lapland, Finland; Privacy Counsel, Cisco Systems, Germany

INTRODUCTION

DATA PRIVACY LAW IN AFRICA: EMERGING PERSPECTIVES

Lukman Adebisi Abdulrauf and Hlengiwe Dube

In Africa today, the right to data privacy¹ faces a considerable challenge as people gradually move many of their daily activities to cyberspace and embrace new digital technologies and the internet.² Indeed, while the steadily-rising internet penetration rates and the uptake of modern technologies across Africa are a welcome development, it is not without a concomitant impact on human rights and fundamental freedoms.³ Africa is now witnessing an era of the proliferation of ubiquitous (data) privacy-intrusive technologies, such as artificial intelligence, advanced surveillance technologies, the internet of things, big data analytics, cloud computing technologies, and the internet itself. All these technologies mean a sharp increase in data processing activities with implications. Unfortunately, the challenges these new technologies pose to human rights and fundamental freedoms are somewhat underestimated on the continent and have been subject to very little academic scrutiny. This issue is one of the key motivations behind this edited volume.

The volume comprises a selection of papers presented at a virtual conference in October 2020 organised by the Centre for Human Rights at the Faculty of Law, University of Pretoria, South Africa. The theme of the conference was 'Privacy and data protection in Africa: Challenges and prospects'. The main objective of the conference was to identify and analyse emerging concerns regarding privacy and data protection in Africa and to suggest ways of overcoming these. Indeed, with the rapid advances in technology worldwide, there is a need to constantly reflect on how emerging technologies constitute a challenge to human rights and

1 Although there have been controversies surrounding the appropriateness of the terms 'privacy', 'data protection' and 'data privacy', these will be interchangeably used in this book to mean the same thing except where a chapter explicitly states otherwise.

2 LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8(1) *Journal of Media Law* 69.

3 J Bryant 'Africa in the information age: Challenges, opportunities, and strategies for data protection and digital rights' (2021) 24 *Stanford Technology Law Review* 389.

fundamental freedoms. This is particularly crucial for a continent grappling with the realisation of human rights in the digital era. It is apposite to state that this volume cannot possibly cover all the emerging challenges to data privacy. However, it attempted to open up the debate on some intricate but overlooked aspects of the subject. Indeed, the discussions around data privacy in Africa should move away from analysing data protection laws and instruments in theory towards discussing how these laws should operate in practice. With more than two decades of experience in data privacy legislative and policy making in Africa, it is time for academics to start debating the law in action. The book is structured in five parts with 12 chapters. Each part contains an analysis and emerging perspective.

Part I: The status of data privacy in Africa

The first part provides an overview of the nature and current status of (data) privacy in Africa. It comprises three chapters.

In chapter 1, entitled ‘A quest for an African concept of privacy,’ Patricia Boshe sets the tone for the discussions by analysing the development of the concept of privacy in Africa. She rightly notes that despite the widely-acclaimed absence of a privacy concept in Africa, the right to privacy has distinctly evolved. Boshe contends that it is crucial to contextually understand the concept’s development in the African setting. This is because of the controversies associated with understanding the difference in conceptual underpinning between the Western and African approaches to privacy. Therefore, African privacy scholars clamour for a distinct African definition of privacy devoid of the general Western trappings of individualism. Boshe points out that in the past decade, privacy has developed on the continent with the adoption and enforcement of legal and regulatory frameworks on information privacy. However, none of these frameworks define or conceptualise privacy for one to understand what it means for Africa. According to her, this challenge could impact the continent’s enforcement of privacy and data protection norms. Boshe, therefore, canvasses the idea that privacy must be conceptualised based on a particular society’s underlying socio-legal and cultural values. From this context, she argues for the need for ‘an alternative approach’ to understanding privacy in Africa based on African communal values depicted in the notions of ubuntu and *ujamaa* and not limited to the Western individualism approach.

Boshe further notes that although the extraterritorial effect of the European Union (EU) Data Protection Directive and the General Data Protection Regulation (GDPR) has forced African countries to adopt frameworks similar to Western-oriented privacy legislation, this move

should not impact the push for an African approach. The requirement that third countries have a similar framework does not mean an 'identical' framework. Therefore, a country can provide a similar level of protection without necessarily adopting identical content. Furthermore, 'the fact that privacy has always been defined to reflect Western cultures is neither a barrier nor an excuse for non-Western cultures to define privacy to reflect specific cultural values and social norms'.

To further appreciate the movement for an African approach to privacy (and data protection) there is a need to track the development of the concept in Africa, given that it is already more than 20 years since the first *sui generis* privacy law appeared on the continent. Chapter 2 by Alex Boniface Makulilo, entitled 'Data privacy in Africa: Taking stock of its development after two decades', provides a broad overview of the development of data privacy laws and policies in Africa. Like Boshe, Makulilo commenced the chapter by analysing the theoretical and philosophical underpinnings of data privacy in Africa and the factors influencing its continental development. He argues that although the risks associated with technological advances were one of the primary reasons for privacy regulations in Western societies, this factor alone may not fully depict the African situation. Makulilo further points out that privacy as a concept originated in Africa with the departure of the colonialists, leaving Africans with constitutions containing privacy protections, among other values. This, according to him, was inconsistent with the collectivist nature of African communities but was nevertheless retained. Within this platform, data privacy legislation began to appear on the continent, starting with Cape Verde in 2001. Since then, over half of the African countries have adopted these *sui generis* data privacy legislation even though the primary regional human rights instrument – the African Charter on Human and Peoples' Rights (African Charter) 1981 – contains no provision on privacy.

Regarding data privacy specifically, Makulilo noted that several determinants influenced the continent's developments. These determinants can be both positive and negative. Factors such as the development of databanks, social media revolutions, fears over privacy threats, and past traumas are positive determinants. The negative determinants include a lack of awareness of privacy risks, transparency resistance, and inadequate legislative consultation. As argued by the author, combining all these determinants resulted in a diversity of policy and regulatory frameworks on data privacy regionally and domestically. An analysis of all these developments by Makulilo demonstrated certain trends in data privacy in Africa. These trends include the fact that data privacy governance is inspired mainly by the EU frameworks and the fact that there is little influence

of African constitutions, continental and regional privacy frameworks. The author established the latter claim by illustrating how African reform processes have mainly been an exercise of ‘copy and paste’, the absence of regional harmonisation, and weak enforcement. Makulilo concluded the chapter by noting that the development of data privacy in Africa still faces critical challenges. However, there are prospects for overcoming these challenges, especially through international cooperation.

One aspect where international cooperation can significantly impact the development of data privacy in Africa is understanding how to balance conflicting rights – in this context, privacy and freedom of expression. Indeed, this is a controversial aspect globally, considering the occasional conflicting objective of both rights, especially in the digital age. Therefore, in trying to understand the nature of the right to privacy and how it should be balanced with freedom of expression in the African human rights system, Yohannes Eneyew Ayalew looked to emerging norms of the African human rights law created at the regional and sub-regional levels. In his chapter titled ‘An old question in a new domain: Some preliminary insights on balancing the right to privacy and freedom of expression in the digital era under the African human rights law’, Ayalew explored two contexts that heighten the conflicts between freedom of expression and privacy in the use of digital technologies. These two contexts are the publication of personal information and an individual’s right to be forgotten. Regarding the former, the issue is centred around publishing personal information about individuals where their private information is posted on the internet. The latter focuses on a situation where there is a need to balance privacy and freedom of expression where a right holder or data subject requests the removal of online content deemed inadequate or incomplete. Ayalew contends that except for South Africa, there is scanty jurisprudence on balancing the right to privacy and freedom of expression on the internet. Therefore, he illustrates how this should be effectively done, drawing lessons from the European human rights system. With regard to the publication of personal information, some factors that have emerged toward balancing after a review of the European jurisprudence include the contribution of personal information to the general debate; the method of obtaining the information; the popularity and prior conduct of the person; the content, form and consequence of publication; and the severity of the sanctions to be imposed. The author, however, cautions that determining which right should take precedence must be on a case-by-case basis.

Part II: Data privacy and artificial intelligence

The chapters in this part of the book gave a glimpse of the nature and status of privacy and data protection in Africa from a general perspective. However, specific issues that constitute data privacy threats are increasing on the continent. Therefore, the second part of the book focuses on the emergence of and increase in the use of artificial intelligence and the challenges it poses to data privacy in Africa. Two chapters deal with this crucial topic. The first, chapter 4, by Emmanuel Salami, titled ‘The ascent of artificial intelligence in Africa: Bridging innovation and data protection’, provides an overview of how artificial intelligence (AI) systems have gained prominence globally and how they process large volumes of personal and non-personal information. This, according to the author, raises profound privacy concerns. He further analysed several instances of deployment of AI systems in various sectors in Africa, including health, finance and service delivery. Instructively, Salami observes that ‘despite the wide usage, the regulation of AI is yet to attract such momentum across the African continent’. Legal instruments with an impact on AI are yet to be fully effective. Salami, thus, assesses the impact of AI systems on the rights to data privacy in Africa, relying on continental, regional and domestic data protection frameworks. He concludes that there is a severe need for Africa and African countries to re-examine their data protection laws, given advances in AI. In this respect, he recommends that African countries must amend some provisions in their laws to align with the demands of contemporary times regarding AI. Furthermore, supervisory authorities must be proactive, especially in issuing guidance documents that can effectively ‘plug new gaps’ identified in the laws, investigate emerging violations and conduct random audits.

The second chapter on data privacy and AI by Moritz Hennemann entitled ‘African data protection laws and artificial intelligence – Regulation, policy, way forward’ focuses on a general analysis of the approach to AI regulation in African data protection laws. In elaborating on the discussions by Salami in the previous chapter, Hennemann engages with considerations that could inform future legal reforms regarding AI in Africa. He acknowledged that the general data protection rules in many African states apply to AI, but pointed out that there is no AI-specific data protection instrument in Africa, both regionally and domestically. The same can be said of the EU, which does not have an AI-specific data protection regulation. Hennemann, however, noted initiatives in this regard in the EU and contends that ‘modifications of EU data protection law to regulate AI specifically are likely’. In considering AI-specific data protection rules, the author notes that such a proposal must balance

threats and opportunities. Therefore, several considerations that emerged from the analysis in the chapter include that in a proposed AI framework, it is important to decide early if a general or sector-specific legislation will be appropriate; and whether consideration should be given to individual privacy or group privacy based on the African philosophy noted earlier in chapters 1 and 2 by Boshe and Makulilo. In addition, a future AI legal proposal for Africa and/or African states must consider the need for social access to data sets for innovation for the general societal good.

Part III: Data privacy and vulnerable groups

The third part of the book examines some of the specific data privacy-related challenges associated with vulnerable groups. This part also acknowledges the difficulty of reconciling the right to privacy with other rights such as the right against discrimination in the digital age. Three incisive chapters focus on this emerging issue. Chapter 6, titled 'Digital vulnerabilities and privacy of children in the digital age in Africa,' authored by Hlengiwe Dube, examined children's vulnerabilities due to exposure to the internet and other digital technologies. According to the author, the vulnerabilities include child grooming; personal information abuse; cyberbullying; sexual exploitation; depression; anxiety; and child trafficking. Dube contends that all these vulnerabilities impact children's privacy. However, discussions on these issues have not been prominent in Africa. Therefore, the author systematically explores children's vulnerabilities in using digital technologies in Africa and the implications on their rights to privacy. In addition, Dube examines the available legal frameworks to determine how much children's rights to privacy are effectively protected in Africa. In doing this, the author reviewed the legal instruments in other jurisdictions, and concluded that the time is now for an 'Africa-specific' approach to the protection of the privacy of children online. Dube, therefore, made crucial recommendations for various stakeholders towards protecting the privacy of children online in the digital age.

In continuation of the discussions on vulnerable groups in Africa, chapter 7, titled 'Gendered digital inequalities: How do we ensure gender transformative law and practice in the age of artificial intelligence in Africa' by Chenai Chair, examines how AI promotes what she refers to as 'gendered digital inequalities'. Using the feminist approach, the author assesses social inequalities affecting women and gender-diverse communities resulting from the way in which data to develop AI is collected, processed and used. Two main issues are addressed in the chapter. The first is the impact of a gender-responsive data protection law on gender transformative law and practice. The second is civil society's role in ensuring gender transformative law and practice. Focusing on the

Southern African Development Community (SADC) region, the author demonstrated the gendered nature of the harms of data processing to marginalised groups. These harms include data concerns related to privacy and gender harms from AI applications. Chair further makes recommendations for civil society towards ensuring gender transformative legal frameworks. According to her, there is a need for context-specific provisions to address harms associated with intersex, transgender and diverse communities in data protection law, which the current legal regimes in SADC and South Africa overlook. Therefore, the author recommends designing and implementing policies that consider the gendered realities of society. Civil society was identified as the appropriate mechanism to champion this course in collaboration with government, academia and technical community stakeholders.

Chapter 8 deals with the peculiar data privacy rights of another set of vulnerable groups using South Africa as a case study. In the chapter titled 'Data protection and privacy for social assistance beneficiaries: A South African perspective' Ncamane Ntando analysed how the adoption of a technological system by the South African Social Security Agency (SASSA) in social grants payment impacts the rights of beneficiaries. He contends that despite the noble objective of this system, which was supposed to accelerate payments, improve efficiency and eliminate fraud, risks remain. According to Ntando, the processing of payment requires the processing of beneficiaries' data with attendant risks. Despite an explicit order of the South African Constitutional Court in *Black Sash Trust v Minister of Social Development* that personal data obtained in the payment of social grant beneficiaries must remain private and not be used for a different purpose, there were still numerous cases of careless use of beneficiaries' data leading to discrepancies in amounts paid. After reviewing the legal framework of social assistance and the protection of data privacy of beneficiaries, the author concludes that there are adequate statutory provisions protecting social grant beneficiaries, but that these provisions are often ignored. According to Ntando, this is disturbing considering the vulnerability of this group of people. The author, therefore, recommends that the protection of beneficiaries' personal information must be prioritised at all stages of the administration of the grant payment system.

PART IV: Data privacy during the COVID-19 pandemic

There is no doubt that the COVID-19 pandemic has significantly impacted every society globally. It has also significantly exposed the vulnerabilities of human rights in times of emergency. Indeed, the right to data privacy has also considerably been threatened by the governments'

and other entities' response to the pandemic. Two chapters in part IV analyse the nature of the challenges to data privacy that emerged in response to COVID-19. The first, chapter 9 by Alex Boniface Makulilo, Rindstone Bilabamu Ezekiel, Doreen Mwamlangala and Mbiki Msumiis titled 'Tracking COVID-19: What are the implications for data privacy in Africa?' provides a general overview of the particular issues posed by the pandemic and their implications for data privacy. The authors noted the use of advanced technologies for contact tracing in many African countries without simultaneous consideration of their implications for data privacy. This situation is even more precarious considering that most information collected is sensitive personal information. The authors reviewed the deployment of various contract tracing applications in Ghana, Kenya, Rwanda, and so forth, and the risks they pose. On the regulatory aspect, the chapter explains global trends that impact data privacy. First, new laws were adopted as existing laws were insufficient in responding to the pandemic. Some of these laws focused on privacy protection using contact tracing applications. Second, there were also amendments to existing (privacy) laws due to the peculiar nature of the challenges of the current time. Third, some countries suspended existing legislation (or rights), obstructing the fight against the pandemic. In the case of Africa, the authors contend that personal health information was collected without sufficient legal protection during the pandemic. The authors conclude that COVID-19 raises issues that a common approach by African states in terms of data privacy could have helped to mitigate.

Chapter 10, titled 'Can we trust Big Brother? The future of COVID-19 research and data protection' is a South African case study of the response to COVID-19 and its impact on the right to data privacy. In the chapter Dusty-Lee Donnelly discussed the data protection implications of the South African government's use of personal data to track citizens and monitor the spread of the virus. The chapter's central question is whether using such data aligns with the data protection objectives of the South African Protection of Personal Information Act (POPIA). To further complicate the uncertainties, the government issued regulations under the Disaster Management Act that provided for the creation of a COVID-19 'contact tracing' database. The issue, according to Donnelly, now turned to how to strike a balance between public emergency and human rights protection. The author analysed the government's response to the pandemic, which included collecting COVID-19 data; creating a COVID-19 tracing database; and guidance from the Information Regulator. She accessed the legality of all these measures contained in several government regulations against the yardstick of the data processing principles in POPIA. The author concluded that the regulations do not substantially comply with POPIA, leading to the next question, namely, whether the non-compliance

can fall into any of the grounds for exception or exemptions, especially the public interest exemption. According to the author, this arguably can fall within the public interest exemption. However, it must be further shown, in terms of POPIA, that public interest to a substantial degree outweighs any interference with the data subject's privacy. This, therefore, creates an onerous criterion to be fulfilled to fall within the public interest exemption. Donnelly further focused on processing such information for health research purposes and a public interest exemption under POPIA. She concludes that the public interest exemption undoubtedly creates a less demanding requirement for processing, and that valuable lessons can be obtained from the South African approach in using data by the government and the legal responses to it.

Part V: Selected data privacy issues from a comparative perspective

While focusing on emerging data privacy issues, the last part of the book (part V) contains comparative discussions. Two issues were the crux of comparative studies – automated decision making (ADM) and profiling and data protection authorities. In chapter 11, titled 'The regulation of automated decision making and profiling in an era of big data and ambient intelligence: A European and South African perspective', Alon Lev Alkalay compares the approaches to the regulation of two pervasive technological developments – ADM and profiling in South Africa and the EU. After unpacking both concepts, the author outlined the ethical and legal issues arising from their use. Some issues identified include algorithmic error; bias and discrimination; information asymmetries; and loss of individual autonomy. Alkalay further conducted an extensive comparative study of the regulation of ADM and profiling under GDPR and POPIA. He showed the two major approaches in which both legal regimes regulate both phenomena and highlighted certain flaws with both approaches. Some of these flaws include a focus on regulating the processing of 'personal' data, which cannot be relied upon to protect data subjects from controllers who generate new knowledge from de-identified and group data; limitations of consent and the transparency principle; the lack of recognition of data mining as a critical source of personal data; and the ineffective notification mechanism when further processing is constituted by data mining. The chapter concluded by recommending, among other things, a shift from regulating 'collection' to 'usage', sui generis law, and external interventions.

All the challenges identified in the preceding chapters mean that Africa must take the right to data privacy very seriously. The issues raised by the various contributors illustrated that it is not enough to merely have

a normative framework (or data privacy laws) in place. There is a need for faithful enforcement and implementation of the normative framework. This points to the role of one significant institution – data protection authorities (DPAs). However, for these institutions to be effective, they must be independent. In acknowledging this fact, chapter 12 by Lukman Adebisi Abdulrauf titled ‘Independence of data protection authorities in Africa: Trends and challenges’ considers the journey so far regarding the application of the concept of independence of DPAs in Africa. Despite the slow pace of establishing DPAs across the continent, this chapter is timely as many of the existing bodies have already swung into action. The chapter reviewed the African standards (both regionally and domestically) on independence against international standards and found that very few countries have sufficiently robust provisions that meet international demands. South Africa is noteworthy in this regard. Abdulrauf further analysed other practical challenges to realising the independence of DPAs in African countries. Among the challenges identified are low awareness of the intricacies of independence’ the shortfall in expertise on the continent; and the general distrust of independent statutory bodies by the ruling class in Africa. The chapter concluded that formal/legal independence and independence in practice must operate side-by-side to achieve real independence by DPAs. In conclusion, Abdulrauf recommends constitutional entrenchment of DPAs, drawing lessons from South Africa with regard to its approach regarding ‘state institutions supporting constitutional democracy’ under chapter 9 of the South African Constitution.

PART I: The status of data privacy in Africa

1

A QUEST FOR AN AFRICAN CONCEPT OF PRIVACY

Patricia Boshe

Abstract

In spite of the absence of a privacy concept in Africa, privacy as a right has evolved. In the past decade Africa has seen the development of privacy with the adoption and enforcement of information privacy legal and regulatory frameworks. This chapter canvasses privacy as a concept and as a right, in general, followed by a discussion on specific issues relating to privacy and data protection in an African context. Privacy being a relatively new concept in Africa, existing privacy perceptions or concepts are analysed through the lens of an African social context and legal culture to determine their fitness *de jure* in Africa. Despite the fact that the right to privacy is a well-known legal concept and a right in the human rights catalogue, African social norms, cultural values and legal culture have an impact on privacy perception. As a result, the strict adoption of any privacy concept or the right to privacy as understood in the Western world may not reflect African social and jural contexts in a way that its interpretation and enforcement constitutes justice. The analyses made on the African Union (AU) legal framework for human rights and, more specifically, data protection enforcement as well as on African social perspectives indicate a desire for an alternative approach to privacy and data protection, other than the Western approach.

1 Introduction

Regimes regulating privacy regulate social behaviours. These regimes are highly influenced by specific culture and social norms. They affect privacy perceptions and its meaning, and they are the foundation of the jurisdictions creating and supporting privacy regimes.¹ This makes

1 D Nelken 'Towards a sociology of legal adaptation' in D Nelken & J Feest (eds) *Adapting legal cultures* (2001) 25-26.

privacy elusive, transitory² and contextual,³ hence difficult to define and to understand. Privacy has different meanings to different people.⁴ It is a concept that ‘has [a] protean capacity to be all things to all lawyers’.⁵ Its meaning may vary and may be determined based on individual interaction with society, culture and technology. Its character is debatable, whether privacy is a state/condition, a claim or a right.⁶ Nevertheless, for jurisprudential reasons it is important to at least understand and describe the interests that privacy protects in order to promote certainty in privacy legislation and enforcement.

This chapter narrates the importance of conceptualising privacy within the context especially of unripe frameworks such as Africa, where privacy is still an abstract concept.⁷ Since 2001 African countries are reforming and developing data protection frameworks, with ‘robust’ and comprehensive frameworks for privacy and data protection – as elaborated in part 3 below. The process has not spared time to define or conceptualise privacy within such frameworks. Despite several calls from African privacy scholars for an African conception of privacy,⁸ there still is neither concept nor theory that uniquely deals with privacy in an African context. Contextualising the privacy concept or theory is not only important in the enforcement of privacy and data protection, but is also inevitable in developing and reforming data protection legal frameworks. So far, privacy takes on the Western idea of what privacy is or should be.⁹ Privacy is regarded as a form of human dignity or personality right. These definitions or privacy concepts are the focus of this chapter. The chapter analyses the current position where privacy and data protection reforms in Africa seem to

2 J Neethling ‘The concept of privacy in South African law’ (2005) 122 *South African Law Journal* 18.

3 JL Cohen ‘What privacy is for’ (2013) 126 *Harvard Law Review* 1904. See also P Boshe ‘Data protection legal reforms in Africa’ PhD thesis, University of Passau, 2017 20, 49, 53-61.

4 Neethling (n 2); see also AR Miller *The assault on privacy: Computers, data banks, and dossiers* (1971) 25; *Bernstein & Others v Bester & Others NNO* 1996 (2) SA 751 (CC) 787-788.

5 T Gerety ‘Redefining privacy’ (1977) 14 *Harvard Civil Rights-Civil Liberties Law Review* 234.

6 LA Bygrave *Data privacy law: An international perspective* (2014) 169.

7 EM Bakibinga ‘Managing electronic privacy in the telecommunications sub-sector: The Uganda perspective’ Africa Electronic Privacy and Public Voice Symposium (2004).

8 The lack of an African privacy concept or theory had been aired out by African privacy scholars such as Bakibinga (n 7) in 2014 and AB Makulilo ‘The context of data privacy in Africa’ in AB Makulilo (ed) *African data privacy laws* (2016) 16.

9 AB Makulilo ‘“A person is a person through other persons”: A critical analysis of privacy and culture in Africa’ (2016) 7 *Beijing Law Review* 192, 196.

have silently and indirectly adopted the Western construction of privacy. The chapter examines the influence of cultures and social norms on the concept, keeping in mind how it has affected (if at all) the privacy and data protection reform agenda in Africa.

Analyses are driven from the assumption that privacy is a universal concept regardless of varied (privacy) cultures and the opposing arguments that no single concept (or two) can describe or denote privacy across cultures. The AU legal framework on the enforcement of human rights and data protection is then analysed in light of the two premises. Eventually, an explanation as to why Africa should conceptualise privacy based on the underlying socio-legal and cultural values is offered. The chapter is the result of a mixture of constructivism and comparative research approaches. The constructivism approach was instrumental for an in-depth examination of the existing social and legal structures and diverse aspects in legal systems. Through constructivism, knowledge was viewed as socially constructed and able to change based on circumstances. This approach was also used to validate diverse realities attached to contexts and legal culture with regard to privacy. A comparative analysis helped in drawing conclusions on the universality and fitness of the existing privacy concept/perceptions in an African context.

2 African privacy: Does it really matter?

An understanding of privacy in a certain context is crucial in regulating interests and values protected and safeguarded by the right to privacy and data protection laws. Bygrave insists that 'the way in which one conceptualises the interests and values served by these laws is not just an academic interest but has significant regulatory implication. It is pivotal to working out the proper ambit of the laws and, concomitantly, the proper mandate for data protection authorities.'¹⁰ Frowein and Peukert emphasise the clarity of the concept, considering the fact that the right to privacy challenged many legal systems of liberal states in the late half of the twentieth century.¹¹ Nevertheless, its understanding is not only crucial in ascertaining its objectives but also affects privacy protection in a given context. Concepts such as privacy are a work of theories and not practice and, therefore, one cannot phrase or derive a concept based on practice,¹²

10 LA Bygrave *Data protection law: Approaching its rationale, logic and limit* (2002) 7. See also Bygrave (n 6).

11 JA Frowein & W Peukert *Europäische Menschenrecht Konvention: EMRK-Kommentar* (1996) 338.

12 P Blume 'Privacy as a theoretical and practical concept' (1997) *International Review of Law Computers and Technology* 194.

no matter how popular such practice is. Concepts are meant to identify and solve practical conflicts, they provoke human mind and underline aspirations and thoughts and, therefore, the most important activity.¹³

Furthermore, diversity in legal cultures¹⁴ and structures, perceptions and an understanding of the right to privacy (or the concept of privacy)¹⁵ have an impact on how a country interprets the basic content and core rules of the law and eventually standards implemented within a specific local jurisdiction.¹⁶ Culture defines law, its purpose, and where and how it is to be found. Arguably, even when the rule is imported, its application is still contextual.¹⁷ Its effectiveness depends on the ability of the interpreter to link the rule with cultural foundations and employ what Krygier refers

13 As above.

14 LM Friedman 'Legal culture and social development' (1969) 29 *Law and Society Review* 35-36. Basically legal culture is the totality of social attitudes, informed by culture and history and countries' institutional characteristics and its legal traditions that give a certain rule a meaning and life.

15 An example on diverging understanding and treatment of privacy and how they impact regulatory standards within certain communities is given by Saad who compares the concept of privacy as perceived in Islamic communities as against the Westerners. In Islamic communities, he said, privacy is aimed at prohibiting public humiliation of the individual even if it is something of a legitimate concern to the public. This is different from the Western concept of privacy that would seem to allow the publication of information of a person's private life if there is legitimate concern. He continues to say that 'even without the existence of law, privacy is a concept recognized in various cultures, but depending on cultural setting, each society has its own attitude and perception towards what amounts to privacy'. AR Saad 'Information privacy and data protection a proposed model for the Kingdom of Saudi Arabia' (unpublished). See also Boshe (n 3) 10.

16 In this context, Tabalujan emphasises that legal culture has an impact on the way in which privacy is perceived and interpreted, which means that social beliefs and norms of the receiving community and the people's willingness and capacity to scour for, understand and obey new laws are important factors that help determine the success of law that is transposed. BS Tabalujan 'Legal development in developing countries: The role of legal culture' (March 2001) 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=268564 (accessed 24 December 2020).

17 JJ Kingsley 'Legal transplantation: Is this what the doctor ordered and are the blood types compatible? The application of interdisciplinary research to law reform in the developing world: A case study of corporate governance in Indonesia' (2004) 21 *Arizona Journal of International and Comparative Law* 495. Law reforms in less developed countries that utilise Western frameworks without adapting or localise such frameworks and ignoring cultural diversity are bound to fail. See also a similar view by A Watson *Legal transplant: An approach to comparative law* (1993) 108 where he insists on the importance of paying attention to a country's legal culture instead of blindly injecting foreign legal theories. See also O Kahn-Freund 'On use and misuse of comparative law' (1974) 37 *Modern Law Review* 6; LM Friedman *The legal system: A social science perspective* (1975).

to as positive sanctions and persuasions to ensure compliance.¹⁸ How law is perceived in one state may differ from the beliefs in another. Blume explains that 'the formal instruments and institutions might be the same, but the differences in the culture imply that the law works or functions in different ways'.¹⁹ This means that an understanding of what privacy means and how it is perceived in Africa is or should be pivotal to any reform process.

The Western understanding of privacy is either a right to be left alone (suggesting an individual claim over one's space or information) or personality right, a right to self-determination or integrity. Looking at the first aspect, simply saying 'right to be left alone' does not say much about the concept. Hickford questioned this definition by saying that it does not clarify content or context – 'left alone how and when?' He states that it presents the possibility of an extreme wide interpretations of situations that may be construed as entailing a right to privacy but may fail to predict the concrete outcomes or when or how to intervene in one case but not in another.²⁰ This means that this construction poses the danger of being interpreted to apply to situations not intended to have been covered at the time of its conception. Bygrave elaborates on privacy by breaking it down into four elements. The first is based on non-interference; the second is based on limited accessibility; the third is based on information control; and the fourth links privacy to intimate or sensitive aspects of a person's life.²¹ This is similar to a meaning given by the Electronic Privacy Information Centre (EPIC) and Privacy International that privacy safeguards four things, namely, personal information; bodily privacy; communications privacy; and territorial privacy.²² This is also similar to what legal scholars have come to agree upon as a form of protection for a liberal self,²³ or self-determination. It is better described by Neethling as the ability of a person to determine his private facts and hence the scope of his interest in privacy, a power that an individual has, that gives a person a right to claim his right to privacy.²⁴

18 M Krygier 'Is there constitutionalism after communism? Institutional optimism, cultural pessimism, and the rule of law' (1996) *International Journal of Sociology* 17-47.

19 Blume (n 1) 194.

20 M Hickford 'A conceptual approach to privacy' Miscellaneous Paper 19/New Zealand Law Commission (October 2007) 19-20.

21 Bygrave (n 6) 70.

22 EPIC 'Privacy and human rights report' (2006), <http://www.worldlii.org/int/journals/EPICPrivHR/2006/> (accessed 20 December 2020).

23 See, eg, C Kuner 'International legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law and Security Review* 308.

24 Neethling (n 2).

Although there is still no universally-accepted definition of privacy, legal scholars and judicial pronouncements seem to have agreed on the scope of privacy. Privacy gives an individual control over their private lives against intrusion, physical or otherwise,²⁵ whether in private, within his intimate space or in social capacity in which people act,²⁶ and it extends to persons' professional activities and certain activities performed in the public sphere.²⁷ As described by Hickford, privacy relates to 'those things or aspects of one's life that you, as an individual in social world, would have a reasonable expectation of exerting control over in terms of dissemination or disclosure should you wish to'. Further, as explained by Moreham:

A person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about. Something is therefore 'private' if a person has a desire for privacy in relation to it: A place, event or activity will be 'private' if a person wishes to be free from outside access when attending or undertaking it and information will be 'private'; if a person to whom it relates does not want people to know about it.²⁸

According to Moreham, privacy is a claim rather than a state or condition of being. It is a claim a person has over his state of affairs, his information and his space that he considers private and intends it to be private. It is a claim of choice; one can choose elements and extent of publicity they desire about themselves. Similarly, Altman believes that privacy is a claim of choice that depends on one's ability to control interaction with others, but he also adds that privacy regulation is a cultural pervasive process.²⁹

As a cultural pervasive process, privacy manages social interaction, establishes plans and strategies for interaction with others and develops

25 See also C Cuijpers 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *SCRIPTed* 312.

26 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smith* NO 2001 (1) SA 545 (CC) 557.

27 See, eg, *Niemitz v Germany* Application 13710/88 16 September 1992 para 29; *Coeriel & Aurik v The Netherlands* (1994) Comm 453/1991 para 10.2, reported in, among others, (1994) 15 HRLJ, 422; P de Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action' in S Gutwirth (ed) *Reinventing data protection* (2009) 15.

28 NA Moreham 'Privacy in the common law: A doctrinal and theoretical analysis' (2005) 121 *Law Quarterly Review* 636; see also Boshe (n 3) 56.

29 I Altman 'Privacy regulation: Culturally universal or culturally specific?' (1997) 33 *Journal of Social Issues* 68.

and maintains self-identity.³⁰ So long as privacy is seen in the context of human interaction, regulating social interchange, its meaning, perception and value are inevitably derived from that particular society. What privacy means in one society cannot be taken to mean the same in another, unless the two societies share history, social and cultural norms that affect the privacy perception. For this reason, scholars such as Cohen believe that privacy should not be viewed as a right because 'the ability to have and manage it depends on the attributes of one's social, material and informational environment'.³¹ At the same time, privacy arguably attends to the body politic to promote civil liberties and, further, fundamental public policy goals relating to liberal democratic citizenship, innovation and human flourishing.³² Consequently, a single formulation of privacy purpose should neither be expected nor should it be viewed as a fixed condition as it changes with individual relationships, social and cultural context in boundary management.³³ Therefore, it is only logical to define or conceptualise privacy by its existence and nature in factual reality.

Certainty on what interests and values privacy or data protection promotes within a specific context is necessary in explaining and discharging supervisory (in case of data protection) and enforcement powers, proportional to, and in safeguarding other societal interests and values in privacy. Unfortunately, even in the Western world, where the right to privacy is relatively developed, there is considerable uncertainty about exactly which interests and values are promoted by data protection laws³⁴ despite extensive researches, publication and in-depth analyses made on the subject.³⁵ As a result, many data privacy laws fail to specify the interests and values they protect.³⁶ Some specify the objectives in general terms, such as the protection of personality or fundamental rights, or as narrow as the protection of personal integrity.

30 Altman (n 29) 29.

31 Cohen (n 3) 9-20.

32 Hickford (n 20) 35.

33 Cohen (n 3) 7.

34 D Korff 'Study on the protection of the rights and interests of legal persons with regards to the processing of personal data relating to such persons' Final Report to the EC Commission (October 1998); see also B Napier 'International data protection standards and British experience' (1992) *Informatica ediritto*; Makulilo (n 9) 195; DJ Solove 'Conceptualising privacy' (2002) 90 *California Law Review* 1087.

35 O Mallmann 'Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information. Mit einer Studie zum Datenschutz im Bereich von Kreditinformationssystemen' (1977) 10 cited in Bygrave (n 9) 172.

36 Bygrave (n 9) 8.

The African regional human rights instrument, the African Charter on Human and Peoples' Rights (African Charter)³⁷ contains no provision on the right to privacy. This omission caused scholars to insinuate that Africa lacks privacy values, arguing that African communalism makes privacy a less important value.³⁸ However, in 2018 the African Union (AU) Commission and the Internet Society published the Guidelines for Personal Data Protection in Africa.³⁹ The Guidelines emphasise the need to have an African understanding of privacy in cognisance of African unique settings. The Guidelines state that '[t]here is a significant cultural and legal diversity across that leads to different privacy expectations and difficulty of formulating and enforcing consistent policy among and sometimes even within member states'.⁴⁰ The need to contextualise privacy had also been advocated in 2004 by Bakibinga, who suggested that '[i]n the myriad of privacy definition and conceptual myopia, there is a need for defining privacy in a way accepted by the society, given the emphasis on communalism versus individualism'.⁴¹

Laws are about the promotion of justice, and justice⁴² is seen in the protection of social interests. It is essential to have an African understanding of privacy to be able to protect those interests. Although privacy regulation arguably is culturally universal, specific behaviours – unique to a particular culture – and techniques used to control interaction

37 African Charter on Human and Peoples' Rights (African Charter) adopted 27 June 1981, OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), entered into force 21 October 1986.

38 LA Bygrave 'Privacy protection in a global context: A comparative overview' (2004) *Scandinavian Studies in Law* 343; Bakibinga (n 7) 2-3; and HN Olinger and others 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *International Information and Library Review* 35-36, who through the concept of Ubuntu explains 'the culture of transparency and openness in *ubuntu* would not understand the need for personal privacy or able to justify it. Thus, personal privacy would rather be interpreted as "secrecy". This "secrecy" would not be seen as something good because it would indirectly imply that the *Ubuntu* individual is trying to hide something, namely her personhood there is little room for personal privacy because the person's identity is dependent on the group. The individualistic cultures of the West argue that personal privacy is required for a person to express his true individuality. With *Ubuntu* individuality is discovered and expressed together with other people and not alone in some autonomous space, and hence personal privacy plays no role in this *Ubuntu* context.'

39 African Union Commission and the Internet Society 'Personal Data Protection Guidelines for Africa' (9 May 2018).

40 As above.

41 Bakibinga (n 7).

42 As justice to a large degree is concerned with living conditions in a broad sense, founded on observation of human behaviour. See Blume (n 14) 193.

– psychological mechanisms used to regulate it – may be quite different from culture to culture.⁴³ Therefore, as Lacey insisted, it is important to contextualise law and legal practices in that ‘legal practices lie not merely in an analysis of doctrinal language but in a historical and social studies of institutions and power relations within which that usage takes place,⁴⁴ especially with privacy, a concept that is hard to define, highly contextual, and with ever-changing value’. Bennett once said that privacy is highly subjective, which means that it varies by time, jurisdiction, ethnic group and gender. To have an acceptable privacy legal framework, the individuals concerned should be those defining the contents of and interests in privacy according to the context.⁴⁵

The argument that law and legal practice on privacy should adhere to factual reality, as Neethling suggested, is based on the knowledge that by nature a person has a fundamental interest in particular facets of their personality (such as their body, good name, privacy, dignity, and so forth). These interests exist autonomously *de facto*, independently of their formal recognition *de jure*.⁴⁶ Consequently, if the jurisprudential concept of privacy is in conflict with its nature *de facto*, it can neither be considered as scientific concept nor can it promote justice. Legal principles based on an inaccurate understanding of factual reality will necessarily lead to uncertainty and contradictions and, consequently, may produce unfair results.⁴⁷

3 Privacy in data protection

Privacy has two dimensions, namely, information privacy and local privacy.⁴⁸ Information or data privacy comprises all ‘personal’ information and facts about an individual, information that requires management in the social world. However, as Hickford elaborates, the term ‘personal information’ should not be confused with ‘private information’ as information may be ‘private’ but not ‘personal’ at all,⁴⁹ and a person may have ‘privacy’ but not the ‘right to privacy’. To have the right to privacy, ‘there must be some valid norms that specifies that some personal information about, or experience of, individuals, should be kept out of

43 Altman (n 29) 68-69.

44 N Lacey *A life of HLA Hart: The nightmare and the noble dream* (2006) 219.

45 C Bennett ‘Information policy and information privacy: International arenas for governance’ (2002) 2 *Journal of Law, Technology and Policy* 386, 389.

46 Neethling (n 2).

47 J Neethling *Persoonlikheidsreg* (1979) 30.

48 Hickford (n 20) 6.

49 As above.

other people's reach'.⁵⁰ Local privacy is the privacy in one's space (control over access to oneself), places inhabited by intimate relationships, places of solitude and those occupied or used in the promotion of personal or professional growth, such as in households, work places as well as in public places.

Data protection as an extension of the right to privacy emerged in the 1970s. At the time scholars insisted on the need to change the terminology and improve privacy protections to suit the changing circumstances. In the Western world, data protection regulations became inevitable with technological development and the emergence of networks that simplified data sharing and eased access to a wider range of personal data. This development also enhanced organisational capacity to collection, share, use and reuse of personal data across organisational boundaries, all of which increased vulnerability in data, and raised security and privacy issues. Although a more or less similar situation arose in Africa, African countries did not adopt frameworks to regulate data usage and information privacy protection. There were no social or academic pressures towards such regulation as in the case of the Western world. The pressure seems to have been brought about by the extraterritorial application of the European Union (EU) framework (initially the 1995 Data Protection Directive (DPD) and the current General Data Protection Regulation (GDPR)). Even South Africa, a country with a longer history in adjudicating the right to privacy than any other African country, stalled with the upgrade from the conventional right to privacy to data protection. It was only in July 2020, 19 years after the first African country adopted a comprehensive data protection framework, that the South African comprehensive framework for data protection came into force.⁵¹

This rationalises arguments that data protection regulations in Africa are an invention of an outside force, not driven from within but from outside. This, in itself, is not a problem. The extraterritorial rules in the DPD and GDPR do not impose an obligation on third countries to adopt a similar framework but rather to provide similar levels of protection. The term 'similar' does not necessarily mean 'identical'.⁵² A country, therefore, may be able to provide a similar level of protection without

50 Hickford (n 20) 40.

51 The law was adopted in 2013, and has been enforced piecemeal. Although substantial provisions entered into force in July 2020 (with a grace period of 12 months) certain provisions relating to the oversight of the access to information will commence on 30 June 2021.

52 M Hennemann 'Wettbewerb der Datenschutzrechtsordnungen Zur Rezeption der Datenschutz-Grundverordnung'(2020) 84 *The Rabels Journal of Comparative and International Private Law* 864.

necessarily adopting identical content.⁵³ Similarly, a country can adopt an identical framework or content and still fail to provide the required levels of protection. In fact, this is the case in Africa. The majority of data protection frameworks adopted an identical framework/content as the EU (either the DPD or the GDPR) but no African country had passed the European Commission adequacy test, neither in the DPD era nor in the current GDPR framework. An adequacy assessment goes beyond a legal text. The assessment looks into the overall framework, the existing supporting system including the political environment, legal and cultural aspects that affect how the substance/content is interpreted and applied. The point is that African countries can have data protection regulations contextualised to specific social contexts and reflect cultural values without copying other frameworks, and at the same time be able to provide for necessary protection within their (African) context and beyond (external adequacy requirements). Legal concepts are neither rigid nor universal and, therefore, can be contextualised to fit underlying social contexts and legal cultures without diminishing fundamental objectives of the law. Blume argues that contextualising concepts is necessary even in the quest for the internationalisation of laws.⁵⁴

In addition, the trends in data protection reforms and development in Africa also suggest existence of a legal challenge. Presently, 20 years after the first African country adopted data protection framework, in an EU style, only 34 out of 55 countries (around 62 per cent) have data protection regulations,⁵⁵ and only 16 of the 33 countries (around 48 per cent) have established enforcement agencies. Furthermore, the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) since its adoption in 2014 has received only 14 signatures and eight ratifications and deposits. According to article 36, to enter into force, the Convention requires at least 15 ratifications and depositions of the ratification instruments at the AU Commission. At the sub-regional level, five of

53 G Greenleaf 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2 *International Data Privacy Law* 68.

54 Blume (n 12) 194.

55 Algeria (2018); Angola (2011); Benin (2009, amended in 2017); Botswana (2018); Burkina Faso (2004); Cape Verde (2001, amended in 2013); Chad (2015); Congo Brazzaville (2019); Côte d'Ivoire (2013); Egypt (2020); Equatorial Guinea (2016); Gabon (2011); Ghana (2012); Guinea (Conakry) (2016); Kenya (2019); Lesotho (2011 gazetted 2012); Madagascar (2014); Mali (2013); Mauritania (2017); Mauritius (2004, amended in 2017); Morocco (2009); Niger (2017, amended in 2019); Nigeria (the 2019 Data Protection Regulation; currently there is a Personal Information and Data Protection Bill of 2020); Rwanda (2020); São Tomé and Príncipe (2016); Senegal (2008, proposal for review made in 2019); Seychelles (2004); South Africa (2013); Togo (2019); Tunisia (2004); Uganda (2019).

the regional economic communities (RECs) have frameworks for data protection.⁵⁶ The regional and sub-regional frameworks and national laws have adopted similar definitions and data protection-related concepts. Although assumed, these laws do not explicitly elucidate whether the adoption of the EU framework and similar data protection concepts also implies the adoption of the underlying privacy concept(s).

4 A myth about African privacy

Popular knowledge is that the right to privacy in Africa is a colonial importation through national constitutions.⁵⁷ This might be true as far as the right to privacy in written form is concerned. However, forms of human rights and individual liberties existed in Africa long before colonisation.⁵⁸ These principles were not in written form because the traditional African legal systems are characterised by unwritten codes. Yet, the law is known by society, enforced through an established mechanism and learnt through observation, in songs, tales and sayings. For this reason, no documentary evidence can be produced as proof. Nonetheless, Frémont mentions the existence of at least one written document enshrining these rights in Africa. He says that in 1236 there was the adoption in *Kouroukan Fuga* (Kanbaga, Mali) of a charter containing human rights. He cites some provisions of the charter, including article 5 which states that '[e]veryone is entitled to life and to the preservation of their physical integrity'.

Frémont states that pre-colonial communities embraced and were tolerant of one another's rights and liberties, as they co-existed.⁵⁹

The fact that many traditional African religions co-existed also suggests the African acknowledgment and respect to human rights and liberties (tolerance). Such rights that existed include liberty of association, freedom of expression, the right to participate in affairs of the state and freedom of circulation. These rights were not conceived and experienced in terms of conflicts, rather, in terms of group rights and of responsibilities.⁶⁰

56 ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, in Abuja on 16 February 2010, followed by EAC Legal Framework for Cyber Laws in 2018-2010, the SADC Data Protection Model Law of 2012 and the ECCAS Model Law and the CEMAC Directive 2013.

57 See Makulilo (n 8).

58 J Frémont 'Legal pluralism, customary law and human rights in Francophone African countries' (2009) 40(1) *Victoria University of Wellington Law Review* 159.

59 Frémont (n 58).

60 K M'Baye *Les Droits de l'Homme en Afrique* (2002) 71-73.

The African human rights system gives rights and imposes duties to one another and to society. This approach is also seen in the current human rights system, an example being articles 18(1) and (2) and chapter II of the African Charter.

The right to privacy introduced in constitutions through bills of rights only complemented (or complicated) local legal systems by creating mixed legal systems (influenced by the Dutch, British, French or Belgians) and superimposed on the existed African traditional legal foundations.⁶¹ As a result, most African countries have pluralistic legal systems, with customary African traditional legal systems,⁶² mixed with a foreign legal system (either common law, civil law, Roman-Dutch or Islamic law).⁶³

The African Charter was adopted 1981 transposing the Universal Declaration of Human Rights (Universal Declaration) but excluded the right to privacy. The assumption is that the omission is based on the 'incompatibility' of the right to privacy as defined under the Universal Declaration.⁶⁴ The definition is in conflict with the spirit of the African Charter. If the right to privacy under the Universal Declaration were to be incorporated under the African Charter without any modification, it would have paralysed the whole idea of the Charter, that is, the promotion of communal values and African cultural norms, in this case, communalism as against individualism. In fact, Ankumah suggests that the African Charter offers little legal protection of individual rights.⁶⁵

A few African countries adjudicated on the right to privacy. In doing so, courts used classic legal remedies from the common law (mostly the law of torts) to provide relief for privacy infringements. South Africa went the extra mile. The South African Constitutional Court in *National Media*

61 Frémont (n 58).

62 P Onyango *African customary law: An introduction* (2013).

63 F Baldelli 'Legal origins, legal institutions and poverty in sub-Saharan Africa' Master's degree thesis, LUISS Guido Carli University, 201020. He argues that 'although colonialism shaped African legal system through legal transplants, erasing large part of customary law, African traditional law continues to persist even after colonialism. Twenty-seven countries in sub-Saharan Africa have a legal system with French civil law influence; sixteen have a British common law system, two have a bi-juridical law system and one, Sudan, applies the Shari'a.' Boshe (n 17) 62.

64 Art 12: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

65 EL Ankumah 'La Commission Africaine des Droits de l'Homme et des Peuples. Pratiques et procédures, Londres' (1995) *Société africaine de droit international et comparé* 189.

*Ltd v Joost*⁶⁶ adopted a description of privacy promulgated by the Supreme Court in the American case of *Griswold v Connecticut*. In this case, privacy is seen as 'a condition which includes all personal facts which a person himself at a relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy'.⁶⁷ This meaning of privacy has since been used and cited in African privacy literary works.⁶⁸

Surprisingly, although the dominant understanding of privacy has American roots, the AU and African countries adopted the EU framework for data protection. The ongoing reforms have neither conceptualised nor contextualised privacy. There also is no express provision on whether privacy takes the European or American form. Much scholarly work emerged during this time, where scholars limited their probing to whether privacy is a concept worth protecting in Africa,⁶⁹ or cementing the fact that privacy in Africa is a Western-imported liberal concept.⁷⁰ Scholars reproduced the same argument that, due to African collectivist culture, data privacy/protection had little chance of success.⁷¹ Another scholar, Gutwirth, argued that a collectivism culture devalues the right to privacy rendering it irrelevant and ineffective in Africa. He believes that Africans view privacy as a foreign right with no basis in an African context, that its meaning is unfitting to African social settings. For the right of privacy to work in Africa, it must be proclaimed by African states and the legal systems.⁷² Most scholars who also believe that privacy is a value recognised, accepted and treasured by Africans are convinced that privacy and data protection enforcement stumbles due to its Western connotations,⁷³ which is unsuited to African social values and legal culture, that is, communalism. Saad states that the dilemma is not on whether African societies recognise and expect privacy, but rather how it is perceived in the African context; that, 'even without the existence of law, privacy is a concept recognised in various cultures, but depending on a cultural setting, each society has its own attitude and perception towards what amounts to privacy'.⁷⁴

66 [1996] 3 SA 262(A) 271.

67 *Griswold v Connecticut* 381 US 479 [1965].

68 Makulilo (n 9) 196; A Roos 'The law of data (privacy) protection: A comparative and theoretical study' PhD thesis, University of South Africa, 2003 554-560.

69 Bygrave (n 11) 328; S Gutwirth *Privacy and the information age* (2002) 24.

70 Makulilo (n 9) 196.

71 Gutwirth (n 69) 24; Bygrave (n 11); Bakibinga (n 7) 2-3.

72 Gutwirth (n 69) 25-26; Boshe (n 17) 18.

73 Bygrave (n 11); Gutwirth (n 69); Olinger (n 11).

74 Gutwirth (n 69).

5 African privacy: A way forward

An understanding of 'African' is a first step towards understanding and defining African privacy. The reception, perception and value of privacy depend on African values and expectations of what privacy should bring. As in the Western world, the way in which privacy is perceived, valued and regulated reflects the existing privacy notions and values. Legal values are construed from social standards, moral values and a long-standing belief of what is important and just. These are the bases of human personality and a very powerful but silent force affecting human behaviour. They reflect moral spirit and contain a judgmental element, involving an individual's idea as to what is right, good and desirable.⁷⁵ In this context, a question once posed by Bygrave is whether privacy is considered an exclusive right to an individual or is also seen to have broader societal benefits.⁷⁶

5.1 Privacy: Understanding the African social context

In Africa, a sense of community overrides a sense of individualism. In fact, an African idea of security and its value depends on personal identification with and within the community. The community, therefore, offers an individual psychological and ultimately security. It is from the community that members receive both physical and ideological identity. The community produces and presents an individual as a community-culture bearer. Since culture is a community property, the community protects it.⁷⁷ It is unlikely for an individual identity to take precedence over community identity. This is not to say that individualism as an ideology and principle of life is completely disregarded. It is discouraged in context of the community; it comes second to the community.⁷⁸ Communalism is reflected in individual consciousness on community needs and rights before 'one-self'. An individual retains a sense of 'individuality' in terms of personal initiatives, a sense of self-reliance,⁷⁹ having their own unique thoughts, ideas, characteristics, accomplishments and private possession.⁸⁰

75 K Sinha 'Essay on values: Meaning, characteristics and importance', <https://www.yourarticlelibrary.com/essay/values/essay-on-values-meaning-characteristics-and-importance/63830> (accessed 30 September 2020).

76 Bygrave (n 11).

77 Boshe (n 3); see also KJ Onipede & OF Phillips 'Cultural values: Index for peace and branding Africa' (2019) *Ladoke Akintola University of Technology* 5.

78 A Olasunkanmi 'Liberalism versus communal values in Africa: A philosophical duel' (2013) *IOSR Journal of Humanities and Social Science* 80.

79 EU Ezedike 'Individualism and community consciousness in contemporary Africa: A complementary reflection' (2005) 8 *African Journal of Philosophy* 2.

80 Olinger (n 38) 296.

That is to say, communalism and individualism co-exist. Yet, as Senghor asserted, it is a system built upon dialogue and reciprocity where the group or the community has priority over the individual without thrashing him, but allowing him to blossom as a person.⁸¹ The African Charter also echoes this aspect by including the word 'peoples' indicating the idea of 'peoplehood', that is, the community. This is in contrast with the superstructure of the Western world which, as Shahadah illustrates it, 'elevates individual over the society and therefore enshrines an ethic of one against others in a situation of existential tension. All institutions of the West predicate their existence on the assertion of an individual as unique even without the group.'⁸²

One may argue that culture is not static. In fact, scholars contend that globalisation and technological development influence cultural changes. Ntibatirirwa, Kimana and Omobowale state that, because of changes in political systems and globalisation, Africans are abandoning their value systems and embrace liberalism and capitalism in support and promotion of individual freedom and autonomy.⁸³ Muduagwu further emphasises that 'globalisation has the potential of eroding national cultures and values and replacing them with the cultural values of more technologically and economically advanced countries, particularly the United States and members of the European Union'.⁸⁴

Shahadah is of a different opinion. He accepts that culture is not static and globalisation and technological development influence cultural changes and impact social values. However, he argues that the shifting dynamics of culture does not mean an alteration in the fundamental principles of the culture. A distinction must be made between practices of the people and their cultural ideals, what he calls 'the superego of the culture'.⁸⁵ That superego remains static. The African cultural superego has always been communalism. Despite the changing dynamics in support of

81 LS Senghor 'Negritude: A humanism of 20th century' (1966) 16 *Optima* 1-8.

82 A Shahadah 'African culture complex', <http://www.africanholocaust.net/africanculture.html> (accessed 1 October 2020).

83 Cited in Makulilo (n 8) 12-13; P Kinani 'When the family become a burden' (1998) *Daily Nations Weekender Magazine*. S Ntibatirirwa 'A wrong way: From being to having in the African value system' in P Giddy (ed) *Protest and engagement: Philosophy after apartheid at an historically black South African university* (2001); AO Omobowale 'The youth and the family in transition in Nigeria' (2006) 16 *Review of Sociology* 85-95.

84 Also cited in Makulilo (n 8) 15; MO Maduagwu 'Globalisation and its challenge to national culture and values: A perspective of a sub-Saharan Africa' in H Köchler and others (eds) *Globality versus democracy? The changing nature of international relations in the era of globalisation* (2000).

85 Shahadah (n 82).

individual ways of life, the level of individualism in Africa still is not the same as that in the Western world.⁸⁶ That is the one thing that creates an entirely different paradigm and behaviour. Communalism informs on the legal culture, which fundamentally informs notions of morality that in turn informs legislation and national hood.⁸⁷ It is the fundamental law. Speaking in the context of African communalism, Desmond Tutu once said that '[w]e are meant to complement each other. All kinds of things go horribly wrong when we break that fundamental law of our being. We say a person is a person through other people. It is not "I think therefore I am". It is rather "I am human because I belong". I participate, I share.'⁸⁸

This explains African notions such as *ubuntu*⁸⁹ and *ujamaa*⁹⁰ which describe African values that place an individual identity within communal solidarity and interdependence.⁹¹ These notions are translated in the African Charter as 'African solidarity'. African solidarity requires an individual to forgo some rights and privileges for the good of the community. Article 29 places a duty on individuals to preserve and strengthen social and national solidarity, African cultural values in relations with other members of the society, and promote and achieve African unity.

Suffice it to say that, in Africa, culture is not only the people, their practices and beliefs; it is the whole process from legal and family to the political level. It instructs life with values and habits that service humanity and has a role in personal continuation. Therefore, African identity is not one hard thing but a multitude of self-imposed conditions, which ideologically run fluidly across indigenous Africa. It is not a scientific observation but a cultural-political one.⁹² Eventually, the African 'legal' system has an ultimate goal of pulling the society together and upholding such cultural values.⁹³

86 Makulilo (n 9) 194.

87 Shahadah (n 82).

88 Archbishop Desmond Tutu quoted in C Banda 'The privatised self? A theological critique of the commodification of human identity in modern technological age in an African context professing ubuntu' (2019) 75 *Theological Studies* 5.

89 A Nguni proverb *umuntu ngumuntu ngabantu* roughly translated as a person is a person through other person, or I am, because we are; and since we are, therefore I am. See further Banda (n 88).

90 A Swahili word and a social policy introduced by the first President of Tanzania, Mwalimu Julius Kambarage Nyerere. It means togetherness, familyhood.

91 Banda (n 88).

92 Shahadah (n 82).

93 Frémont (n 58) 162.

5.2 Privacy concept and regulation in Africa: A proposal

Communalism also exists and has survived globalisation and technological changes in other parts of the world, such as in Latin America and the Far East. Similar to African communities, they have community-oriented cultures that emphasise 'denial of self'. As such, having privacy as a concept that protects an individual autonomy brings about value conflicts.⁹⁴ Capurro illustrates this in the context of Japan where in 1964 the Western notion of privacy was introduced and made a legal term. Although adopted from the Western world, privacy is perceived differently from in the Western world. In Japan privacy is perceived as a 'crisis of privacy issue' and not as the basis for democratic concern as in the Western world. It takes a form of 'self' within a group dynamic.⁹⁵ In China⁹⁶ privacy is protected in a social context, in consideration of social security and the stability of the social order. The emphasis rather is on the interests of the nation and society than on the individual, although an individual still has a right to privacy.⁹⁷ Similar to the position in Japan and China, in Africa an individual's privacy is recognised as secondary to community rights and interests.⁹⁸

The fact that privacy has always been defined as reflecting Western cultures is neither a barrier nor an excuse for non-Western cultures to define privacy to reflect specific cultural values and social norms. In fact, even in the Western world the concepts and legal frameworks regarding the protection of privacy differ. On the one hand, privacy as initially defined in the US gives a person a right to define and limit access to his space – the right to be left alone. Eventually, privacy policies have a central role in securing a person's 'aleness'. In the words of Bygrave, the US privacy has a goal of securing individuality and achieving individual goals of self-realisation against the need of a wider society.⁹⁹ On the other hand, the European approach is more or less the promotion of personality rights, that is, the right to self-determination, personal identity, integrity and personal development. In terms of the regulation, the US takes a

94 R Capurro 'Privacy: An intercultural perspective' (2005) *Ethics and Information Technology* 37.

95 R Capurro 'Intercultural aspects of digitally mediated whoness, privacy and freedom' in R Capurro and others *Digital whoness: Identity, privacy and freedom in the cyberworld* (2013) 217.

96 See A Geller 'How comprehensive is Chinese data protection law? A systematisation of Chinese data protection law from a European perspective' (2020) 69 *GRUR International* 1191.

97 Geller (n 96) 223.

98 See Malabo Convention in ch II sec I art 2.

99 Bygrave (n 11) 171.

sectoral approach in combination with co-regulatory schemes while Europe adopts a comprehensive regulatory approach. The GDPR recently introduced co-regulatory approaches to complement the comprehensive regulation.¹⁰⁰ This also demonstrates that frameworks regulating privacy and data protection are contextual as well as revolving based on societal underlying interests and what justice is in a given time and place.¹⁰¹

African solidarity is an important aspect not only in understanding privacy perceptions but also in conceptualising and regulating privacy and related rights. There is a need for an approach to privacy that reflects African solidarity instead of submerging it, to avoid 'creating' or adopting a right or a legal framework that is incompatible with or where its enforcement undermines the spirit of the regional human rights charter. Narrating the importance of solidarity in African law making, Frémont states that 'the duty of solidarity has played and continues to play a major role in the establishment of behavioural norms, which are usually very constraining. For all purposes, they organise the life of the family, the clan and the village. The translation of such solidarities, ideally, should be found in legal norms.'¹⁰²

An alternative approach to privacy, such as relational privacy, where privacy is a right enforced in view of or in relation to other community rights and duties, may be adopted. Lassiter once reiterated that in Africa an 'individual's existence and identity is relative to the group and is defined by the group. The strong collective thinking of ubuntu implies that the individual members of the group cannot imagine ordering their lives individualistically without the consent of their family, clan or tribe.'¹⁰³ In the alternative, a form of group privacy, as a conditional right in view of one's community, can be developed. This approach would also seem to be implied by the Malabo Convention – in data protection and the African Charter – as an approach to human rights enforcement in Africa.

100 Art 42 of the GDPR that encourages member states to create certification mechanisms in demonstrating compliance with the Regulation; also art 40 encouraging the drafting of codes of conduct for the implementation of the regulation in specific sectors or for specific needs. Art 27 of the 1995 EU Data Protection Directive that was replaced by GDPR.

101 On factors influencing approaches to privacy and data protection policies and regulatory framework in Bygrave (n 11) 177.

102 Frémont (n 58) 150.

103 JE Lassiter 'African culture and personality: Bad social science, effective social activism, or a call to reinvent ethnology?' (2000) *African Studies Quarterly* 5; quoted in Makulilo (n 9) 194.

The African Charter not only envisions the promotion and protection of group or community rights, but requires human rights enforcement to take into account histories and African values in conceptualising human and peoples' rights in Africa. The Preamble states:

Taking into consideration the virtues of their historical tradition and the values of African civilisation which should inspire and characterise their reflection on the concept of human and peoples' rights;

[Member states] firmly convinced of their duty to promote and protect human and peoples' rights and freedoms taking into account the importance traditionally attached to these rights and freedoms in Africa.

Specifically on data protection, the Malabo Convention states in Preamble 12 that one of its goals is to see the enforcement of the rights – within the Convention – in cognisance of among other things, community rights.¹⁰⁴ Such a framework should not only secure personal information and support knowledge economy, but also reflect the African cultural, legal and social context.¹⁰⁵

Furthermore, chapter II section I article 2 of the Convention states:

The mechanism so established [for protection of data and punish any violation of privacy] shall ensure that any form of data processing respects the fundamental principles and rights of natural persons while recognising the prerogatives of the State, the rights of the local communities and the purposes for which businesses were established.

104 The Preamble states: 'Considering that the goal of this Convention is to address the need for harmonised legislation in the area of cyber security in Member States of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use; that by proposing a type of institutional basis, the Convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses; and take on board internationally recognized best practices.'

105 Preamble 9 of the Malabo Convention: 'Convinced that the afore-listed observations justify the call for the establishment of an appropriate normative framework consistent with the African legal, cultural, economic and social environment; and that the objective of this Convention is therefore to provide the necessary security and legal framework for the emergence of the knowledge economy in Africa.'

The suggested approach would mean that the enforcement of the individual right to privacy takes into account existing privacy-related group rights without necessarily affecting any privacy rights of an individual. It means, as well elaborated by Floridi, that 'any defence of personal privacy must also take into account moderate group privacy, for affecting the latter does mean affecting the personal privacy of its members'.¹⁰⁶ It is a framework that expresses the desires put forward by the African Charter and the Malabo Convention to support African solidarity; a desire to maintain social identity and personhood as understood within the African context. The essence of group privacy is to protect individual privacy without completely secluding that individual from the group or without forcing a person to abandon the group and to stand alone as an individual.¹⁰⁷ It upholds the integrity of the social structure. As Bloustein clarifies:

Group privacy is an extension of individual privacy. The interest protected by group privacy is the desire and need of people to come together, to exchange information, share feelings, make plans and act in concert to attain their objectives ... Individual privacy by regulating whether, and how much of, the self will be shared; group privacy is fashioned by regulating the sharing or association process.¹⁰⁸

The idea of enforcing group rights is not a new phenomenon. The first human rights documents, the Universal Declaration and the International Covenant on Civil and Political Rights (ICCPR), listed rights that should not be curtailed irrespectively of whether it concerned the liberties of individuals, groups or even legal persons. According to Taylor, the main idea behind these documents was not one of granting subjective rights to natural persons, but rather laying down minimum obligations for the use of power by states. Consequently, states, legal persons, groups and natural persons could complain if the state exceeded its legal discretion.¹⁰⁹

Enforcing privacy in relation to relational privacy or as part of a group (group privacy) would reflect the spirit of the African Charter and an African approach to human rights enforcement, that is, rights must correspond to duties and interests of society – the group. The enforcement

106 L Floridi 'Group privacy: A defence and an interpretation' in L Taylor, L Floridi & B van der Sloot (eds) *Group privacy: New challenges of data technologies* (2017) 113.

107 EJ Bloustein 'Group privacy: The right to huddle' (1977) 8 *Rutgers Camden Law Journal* 222.

108 As above.

109 L Taylor and others 'Introduction: A new perspective on privacy' in Taylor and others (n 106) 18.

framework could incorporate or recognise communal groups (to include rights-based organisations such as consumer protection groups) as well as community elders – when applicable – as having *locus standi* in privacy litigations to represent the group (privacy) interests. In this case, the adjudging authority is in a position to assess and balance the individual and group rights; in the words of the Malabo Convention, to give cognisance of the community rights in the enforcement of individual rights.

6 Conclusion

Privacy and data protection regulations are necessary even in Africa where many legal scholars believe privacy to have no value, is irrelevant and its regulation is ineffective. Despite communalism, privacy has value in Africa. Furthermore, African countries face similar data vulnerability, privacy and security issues as in the rest of the world. The lack of a reference to privacy in the African Charter is neither an implication nor an evidence of a lack of privacy values in Africa, but rather could be construed as a possible conflict in the underlying concept.

In 2001, when African states embarked on the data protection legal reform journey, they did so unpreparedly. The African Charter had not ‘recognised’ privacy as a human right. Despite its judicial enforcement in some of African countries, privacy had not been ‘embraced’ as a fundamental human right. Nevertheless, states adopted the EU data protection framework to sustain trade while figuring out where Africa stands. Yet, 20 years later, data protection enforcement is stalling, and there still is no privacy concept or philosophy. Nonetheless, the Malabo Convention, the African Privacy Guidelines and some of the RECs’ data protection frameworks illustrate the presence of an African philosophy/concept of privacy or at least an African approach to privacy. They also emphasise the need to translate the already-adopted data protection frameworks to reflect that ‘philosophy/concept of privacy’. Nevertheless, what African privacy entails is not expressly and clearly presented in any of these documents.

The AU, by suggesting the existence of an African privacy, has a corresponding duty to present a ‘suitable’ privacy concept or philosophy. This is important not only for juridical reasons but also for setting standards that will define privacy in Africa in the future, to provide a firm legal consensus on the exact values and interest that privacy promotes in an African context, lest Africa is subjecting itself to adopting whatever privacy concepts, philosophies and regimes that would, in the future, dominate the discourse. A blueprint for conceptualising privacy as

presented in exists in legal texts – both at the AU as well as RECs – could be used to conceptualise privacy in Africa.

References

- Altman, I 'Privacy regulation: Culturally universal or culturally specific?' (1997) 33(3) *Journal of Social Issues* 66
- Ankumah, EL *La Commission africaine des droits de l'homme et des peuples. Pratiques et procédures* (Londres Société africaine de droit international et compare, 1997)
- Bakibinga, EM 'Managing electronic privacy in the telecommunications sub-sector: The Uganda perspective' (2004) A paper presented at *Africa Electronic Privacy and Public Voice Symposium* held on December 6, 2004, Cape Town, Republic of South Africa, available online at <http://thepublicvoice.org/events/capetown04/bakibinga.doc> (accessed 30 September 2020)
- Baldelli, F 'Legal origins, legal institutions and poverty in sub-Saharan Africa' Master's degree thesis, LUISS Guido Carli University, 2009/2010
- Banda, C 'The privatised self? A theological critique of the commodification of human identity in modern technological age in an African context professing ubuntu' (2019) 75 *Theological Studies* available online at <https://www.scielo.org.za/pdf/hts/v75n1/19.pdf> (accessed 30 September 2020)
- Bennett, C 'Information policy and information privacy: International arenas for governance' (2002) 2 *Journal of Law, Technology and Policy* 386
- Bloustein, EJ 'Group privacy: The right to huddle' (1977) 8 *Rutgers Camden Law Journal* 219
- Blume, P 'Privacy as a theoretical and practical concept' (1997) 11 *International Review of Law Computers & Technology* 193
- Bygrave, LA 'Privacy protection in a global context: A comparative overview' (2004) 47 *Scandinavian Studies in Law* 319
- Bygrave, LA *Data privacy law: An international perspective* (Oxford University Press 2014)
- Bygrave, LA *Data protection law: Approaching its rationale, logic and limit* (Kluwer Law International 2002)
- Capurro, R 'Intercultural aspects of digitally mediated whoness, privacy and freedom' in Capurro, R and others *Digital whoness: Identity, privacy and freedom in the cyberworld* (Ontos Verlag 2013), 211
- Capurro, R 'Privacy: An intercultural perspective' (2005) 7 *Ethics and Information Technology* 37
- Christen, M & Loi, M 'Two concepts of group privacy' (2020) 33 *Philosophy and Technology* 207
- Cohen, JL 'What privacy is for' (2013) 126 *Harvard Law Review* 1904

- Cuijpers, C 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *Scriptorium* 304
- Davidson, B *The African genius* (James Currey 1969)
- De Hert, P & Gutwirth, S 'Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action' in Gutwirth S and others (eds) *Reinventing data protection* (Springer 2009), 3
- Ess, C 'Lost in translation? Intercultural dialogues on privacy and information ethics' (2005) 7 *Ethics and Information Technology* 1
- Ezedike, EU 'Individualism and community consciousness in contemporary Africa: A complementary reflection' (2005) 8 *African Journal of Philosophy* 59
- Floridi, L 'Group privacy: A defence and an interpretation' in Taylor, L, Floridi, L & Van der Sloot, B (eds) *Group privacy: New challenges of data technologies* (Springer, 2017), 83
- Freedman, LM 'Legal culture and social development' (1969) 4 *Law and Society Review* 29
- Frémont, J 'Legal pluralism, customary law and human rights in Francophone African countries' (2009) 40 *Victoria University of Wellington Law Review* 149
- Friedman, LM *The legal system: A social science perspective* (Russell Sage Foundation 1975)
- Frowein, JA & Peukert, W *Europäische Menschenrechts Konvention: EMPK-Kommentar* (Engel, Norbert 1996)
- Geller, A 'How comprehensive is Chinese data protection law? A systematisation of Chinese data protection law from a European perspective' (2020) 69 *GRUR International* 1191
- Gerety, T 'Redefining privacy' (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 233
- Golafshani, N 'Understanding reliability and validity in qualitative research' (2003) 8 *Qualitative Report Volume* 597
- Greenleaf, G 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2 *International Data Privacy Law* 68
- Gutwirth, S *Privacy and the information age* (Oxford 2002)
- Hennemann, M 'Wettbewerb der Datenschutzrechtsordnungen Zur Rezeption der Datenschutz-Grundverordnung'(2020) 84 *The Rabels Journal of Comparative and International Private Law* 864

- Hickford, M 'A conceptual approach to privacy' (2007) *Miscellaneous Paper 19/ New Zealand Law Commission*
- Johnson, SD 'Will our research hold up under scrutiny?' (1995) 23 *Journal of Industrial Teacher Education* 3
- Kahn-Freund, O 'On use and misuse of comparative law' (1974) 37 *Modern Law Review* 1
- Kinani, P 'When the family becomes a burden' (1998) *Daily Nations Weekender Magazine*
- Kingsley, JJ 'Legal transplantation: Is this what the doctor ordered and are the blood types compatible? The application of interdisciplinary research to law reform in the developing world: A case study of corporate governance in Indonesia' (2004) 21 *Arizona Journal of International and Comparative Law* 494
- Korff, D 'Study on the protection of the rights and interests of legal persons with regards to the processing of personal data relating to such persons' Final Report to the EC Commission (October 1998)
- Krygier, M 'Is there constitutionalism after communism? Institutional optimism, cultural pessimism, and the rule of law' (1996) 26 *International Journal of Sociology* 17
- Kuner, C 'International legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law and Security Review* 307
- Lacey, N *A Life of HLA Hart: The nightmare and the noble dream* (Oxford University Press 2006)
- Lassiter, JE 'African culture and personality: Bad social science, effective social activism, or a call to reinvent ethnology?' (2000) 3 *African Studies Quarterly* 1
- Maduagwu, OM 'Globalisation and its challenge to national culture and values: A perspective of a sub-Saharan Africa' in Köchler, H *Globality versus democracy? The changing nature of international relations in the era of globalisation* (Vienna 2000) 213
- Makulilo, AB "'A person is a person through other persons": A critical analysis of privacy and culture in Africa' (2016) *Beijing Law Review* 192
- Makulilo, AB 'The context of data privacy in Africa' in Makulilo, AB (ed) *African data privacy laws* (Springer 2016) 3
- Matondo, MJ 'Cross-cultural values comparison between Chinese and sub-Saharan Africans' (2012) 3 *International Journal of Business and Social Science* 38
- Mbaye, K *Les Droits de l'Homme en Afrique* (Editions A Pedone 2002)
- Miller, AR *The assault on privacy* (University of Michigan Press 1971)

- Moreham, NA 'Privacy in the common law: A doctrinal and theoretical analysis' (2005) 121 *Law Quarterly Review* 636
- Napier, B 'International data protection standards and British experience' (1992) *Informatica ediritto* 83
- Neethling, J 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18
- Nelken, D 'Towards a sociology of legal adaptation' in Nelken D & Feest J (eds) *Adapting legal cultures* (Hart Publishing 2001) 7
- Ntibagwirwa, S 'A wrong way: From being to having in the African value system' in Giddy, P (ed) *Protest and engagement: Philosophy after apartheid at an historically black South African university* (Washington 2001) 65
- Olasunkanmi, A 'Liberalism versus communal values in Africa: A philosophical duel' (2013) 12 *IOSR Journal of Humanities and Social Science* 78
- Olinger HN and others 'Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *International Information and Library Review* 31
- Omobowale, LS 'The youth and the family in transition in Nigeria' (2006) 16 *Review of Sociology* 85
- Onipede, KJ & Phillips, OF 'Cultural values: Index for peace and branding Africa' (2019) (Conference paper)
- Onyango, P *African customary law: An introduction* (LawAfrica Publishing Limited 2013)
- Posner, RA 'An economic theory of privacy' in Shoeman, FD *Philosophical dimensions of privacy: An anthology* (Cambridge University Press 1984) 333
- Reviglio, U & Alunge, R '"I am datafied because we are datafied": An ubuntu perspective on (relational) privacy' (Springer 2020)
- Roos, A 'The law of data (privacy) protection: A comparative and theoretical study' PhD thesis, UNISA, 2003
- Saad AR 'Information privacy and data protection a proposed model for the Kingdom of Saudi Arabia' (unpublished)
- Senghor, LS 'Negritude: A humanism of 20th century' (1966) 16 (1) *Optima* 1
- Shahadah, A 'African culture complex', <http://www.africanholocaust.net/africanculture.html> (accessed 1 October 2020)
- Sinha, K 'Essay on values: Meaning, characteristics and importance', <https://www.yourarticlelibrary.com/essay/values/essay-on-values-meaning-characteristics-and-importance/63830> (accessed 30 September 2020)

Solove, DJ 'Conceptualising privacy' (2002) 90 *California Law Review* 1087

Tabalujan, BS 'Legal development in developing countries: The role of legal culture' (March 2001), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=268564 (accessed 24 December 2020)

Taylor, L and others 'Introduction: A new perspective on privacy' in Taylor, L and others (eds) *Group privacy: New challenges of data technologies* (Springer 2017) 1

Watson, A *Legal transplant: An approach to comparative law* (University of Georgian Press 1993)

2

DATA PRIVACY IN AFRICA: TAKING STOCK OF ITS DEVELOPMENT AFTER TWO DECADES

Alex Boniface Makulilo

Abstract

Exactly two decades have lapsed since the first data protection legislation in Africa was enacted (in Cape Verde). This chapter aims to offer a broad overview of the development of data privacy laws and policies in Africa. The theoretical and philosophical underpinnings of data privacy in Africa as well as factors that have influenced this development are considered. The future development of data privacy in Africa is finally projected against that particular background. The chapter is divided into the following parts: Part 1 provides a general overview of data privacy globally. Part 2 covers the African world view on privacy. Part 3 considers determinants of privacy concerns in Africa over the past two decades. Part 4 provides legal and policy frameworks of data privacy in Africa. Part 5 provides a discussion of the patterns and trends of data privacy policies. Part 6 concludes the chapter.

1 Introduction

Privacy is a Western concept. It has evolved over the years. Bennett observes that record keeping on individuals (one of the reasons why data privacy laws partly emerged to regulate) is as old as civilisation itself.¹ The Roman Empire, for example, maintained an extensive system of taxation records on its subjects, who were identified through census taking.² However, the modern conception of privacy and data protection may be traced from Warren and Brandeis's seminal article 'The right to

1 CJ Bennett *Regulating privacy: Data protection and public policy in Europe and the United States* (1992) 18.

2 A Roos 'The law of data (privacy) protection: A comparative and theoretical study' LLD thesis, UNISA, 2003 1-2. See also A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 402. It is worth noting that the most extreme example of census abuse is Hitler's use of the census to track minorities for extermination during the Nazi regime. See EPIC 'The census and privacy', <http://epic.org/privacy/census/> (accessed 10 November 2021). For more discussion about privacy risks associated with population census, see also the famous census judgment of the German Federal Constitutional Court in 1983, Federal Constitutional Court, Judgment of 15 December 1983, 1 BvR 209/83.

privacy', published in the *Harvard Law Review* in 1890.³ This article indeed is increasingly acknowledged by commentators as the official birth date of the right to privacy in the world.

It is worth noting that in the 1960s and 1970s concrete privacy and data protection regulations emerged in North America and Europe. This is not surprising as the rise of computer technology around that time increased many possibilities with which organisations, both public and private, as well as individuals could process personal information in ways that could interfere with an individual's privacy. The legal response to the rise of computer technology with respect to the protection of an individual's privacy had been to enact data protection legislation.⁴ While technological factors occupied the central role in the emergence of data protection laws, there were other factors that operated as catalysts for such an emergence. Bygrave discusses three main catalysts for emergence of data protection laws: first, technological-organisation trends (growth in amount of data stored and their integration; increased sharing of data across organisational boundaries; growth in re-use and re-purposing of data; increased risk of data misapplication; information quality problems; and diminishing role of data subjects in decision-making processes affecting them); second, public fears (fears over threats to privacy and related values and restriction in transfer of personal data and thereby in goods and services); and, third, legal factors (influence of international human rights instruments proclaiming rights to privacy as well as insufficiency of protection of privacy under existing rules).⁵ In 2004 Bygrave expanded on this list to include ideological factors as essential in determining privacy levels. Central among these are attitudes to the value of private life, attitudes to the worth of persons as individuals, and sensitivity to human beings' non-economic and emotional needs.⁶ Bygrave notes that the concern over privacy tends to be high in societies espousing liberal ideals.⁷

3 SD Warren & LS Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review*. 193-195. This work has frequently and traditionally been cited in numerous scholarly writings on the history of the right to privacy.

4 The first data protection law in the world was adopted by the German *Land* of Hesse in October 1970. Then followed Sweden (1973); the United States (1974); Germany (1977); France, Denmark and Austria (1978); Luxemburg (1979); New Zealand (1982); the United Kingdom (1984); Finland (1987); Ireland, Australia, Japan and The Netherlands (1988). Today almost all Western countries have adopted data protection legislation.

5 LA Bygrave *Data protection law: Approaching its rationale, logic and limits* (2002) ch 6.

6 LA Bygrave 'Privacy protection in a global context – A comparative overview' (2004) 47 *Scandinavian Studies in Law* 328.

7 As above.

However, modern privacy and data protection challenges arise mainly from globalisation, technological progress (for instance, big data analytics, cloud technology, internet of things, artificial intelligence (AI)) and seamless cross-border flows of personal data. It is important to note that every region of the world (Europe, America, Asia, Australia, Africa) is experiencing such challenges. Of course, the magnitude and effect of such challenges differ significantly due to a wide range of factors. Generally speaking, the more a particular society is exposed to technology and associated risks to abuse of personal data, the more such society is likely to raise privacy concerns and demands for its regulation. However, this might not well explain the origins of the concept privacy in most African independent constitutions towards the end of the colonial period in Africa. As Makulilo argues, the concept of privacy developed in Africa at the end of the colonial period, particularly as outgoing colonial powers often left behind constitutions providing protections of privacy, among other values, even though this may have been inconsistent with the more collectivist values of those societies at the time.⁸ Despite that, the first data protection legislation on the African continent appeared in Cape Verde in 2001. Since then, other African countries have adopted data privacy laws and policies. Until February 2021 about 30 African states out of 55 (see figure 1)⁹ had enacted data protection legislation laws that are closely aligned to the first generation of data privacy laws (that is, the OECD Guidelines 1980 and Council of Europe Convention 1981) and second generation of data privacy laws (that is, EU Directive 95/46/EC). Since 2016 new data protection legislation and revision in Africa have largely been aligned to the third generation of data privacy laws, namely, the EU General Data Protection Regulations 2016 (GDPR).¹⁰ It is worth mentioning that the Council of Europe Convention 108+, which is also part of the third

8 AB Makulilo 'The quest for information privacy in Africa' (2018) 8 *Journal of Information Policy* 324-327.

9 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Congo-Brazzaville, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea Conakry, Côte d'Ivoire, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, São Tomé and Príncipe, Senegal, Seychelles, South Africa, Togo, Tunisia and Uganda. As of 2024, about six more countries have enacted data protection law making the total figure to be 36 countries with data protection laws in Africa.

10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980; the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS 108), 1981; the General Data Protection Regulation 2016/679 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 2018.

generation of data privacy laws, has slowly started to exert its influence in Africa following the first accession by Mauritius on 4 September 2020.

This chapter offers a broad overview of the development of data privacy laws and policies in Africa. The theoretical and philosophical underpinnings of data privacy in Africa and the factors that have influenced this development are considered. The future development of data privacy in Africa is finally projected against that particular background. The chapter is divided into the following parts: Part one provides a general overview of data privacy globally. Part two covers the African worldview on privacy. Part three considers determinants of privacy concerns in Africa over the past two decades. Part four provides legal and policy frameworks for data privacy in Africa. Part five discusses the patterns and trends of data privacy policies. Part six concludes the chapter.

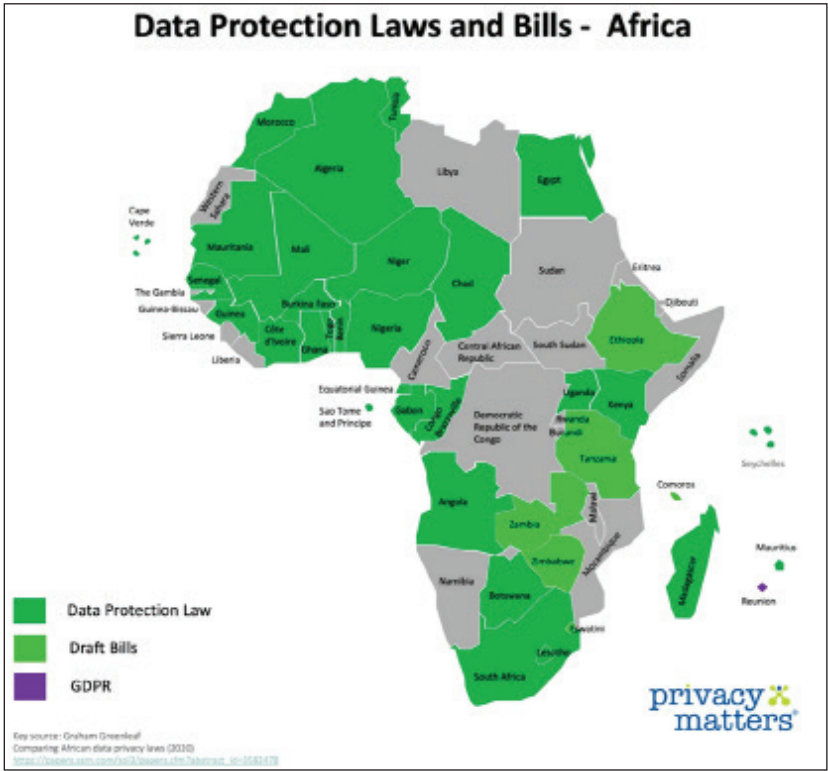


Figure 1 shows the state of data protection laws in Africa as of February 2021.

2 The African world view on privacy

2.1 Privacy notion

In their seminal article ‘The right to privacy’, renowned legal scholars Warren and Brandeis defined privacy as ‘the right to be let alone’. Since this time, different legal and non-legal scholars have conceptualised privacy in different formulations. This chapter does not intend to review debates around the definition of privacy. However, one important point about the various schools of thought is that there yet is no consensus as to the acceptable definition of the notion ‘privacy’. Nonetheless, the bottom line of most of the definitions is individualism. That is, privacy is an individual right. Its normative basis is spelt out in international and regional human rights instruments, such as article 12 of the Universal Declaration of Human Rights 1948 (Universal Declaration); article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR); article 8 of the European Convention on Human Rights 1950 (European Convention); article 17 of the Arab Charter on Human Rights 1994 (Arab Charter); and article 5 of the American Declaration of the Rights and Duties of Man 1948. Surprisingly, the African Charter on Human and Peoples’ Rights (African Charter) does not contain a specific provision for the protection of privacy. Because of this, commentators such as Gutwirth argues:

Insofar as sub-Saharan Africa can be assessed as one whole, privacy stands for little. Notably, the 1981 African Charter on Human and Peoples’ Rights does not even mention privacy ... The Charter highlights African values and traditions, which give content and meaning to human rights. It centres on community, whether this is family, a group, or a people. The individual cannot fully rely on human rights when faced with the group or state ... The status of individual is limited ... Individualism is subordinate to the group, reducing the space for privacy. In practice, the dominance of the collective spirit probably even exceeds the boundaries set by the Charter. This is so, even though many African states shortly after obtaining independence partially or fully adopted the legal system of their colonizers, which was based on the individual.¹¹

Bygrave similarly argues:

The liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection. These regimes are most comprehensive in Western liberal democracies ... By contrast, such regimes are under-developed

11 S Gutwirth *Privacy and the information age* (2002) 24.

in most African and Asian nations. It is tempting to view this situation as symptomatic of a propensity in African and Asian cultures to place primary value on securing the interests and loyalties of the group at the expense of the individual. However, care must be taken not to paint countries and cultures into static categories. As elaborated in section 5 below, provision for privacy rights is increasingly on the legislative agenda of some African countries. A similar development is occurring in some Asian jurisdictions.¹²

Following some privacy and data protection policy developments in Africa, particularly the adoption of data privacy policies, Bygrave has argued:

Until recently, African organizations scarcely figured as policy entrepreneurs in the field of data privacy. The situation today is different. Africa is now a home to some of the most prescriptively ambitious data privacy initiatives at the regional and sub-regional levels. The leading initiative comes from the 15 members of ECOWAS. It takes the form of Supplementary Act on Protection of Personal Data within ECOWAS, adopted in 2010.¹³

Despite the development of privacy laws and policies in Africa, there is neither concept nor theory that distinctly deals with privacy in an African cultural context. The specific call for the conceptualisation of privacy in an African context appears only in the works of Bakibinga. As pointed out, Bakibinga holds that an individual in Africa can have privacy and still be part of the community.¹⁴ Building upon this premise, she makes a definitive call specifically on Uganda that privacy has to be defined in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights.¹⁵ She further contends that privacy should not remain an abstract, and one way to start would be to commission studies to obtain perceptions of privacy within Ugandan society.¹⁶

Currently, the only theory of privacy that has gained prominence in Africa, albeit not in the African cultural context as such, is that of a

12 Bygrave (n 6) 328.

13 LA Bygrave *Data privacy law: An international perspective* (2014) 80.

14 EPIC Alert 'EPIC hosts privacy and public voice conference in Africa' (23 December 2005) Vol 11, No 24, http://www.epic.org/alert/EPIC_Alert_11.24.html (accessed 10 November 2021).

15 EM Bakibinga 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective' 2004 4, <http://thepublicvoic.org/eventscapetown04/bakibinga.doc> (accessed 10 November 2021).

16 As above.

renowned professor, Johann Neethling. Neethling's theory of privacy states:

Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy.¹⁷

The above definition of privacy implies an absence of acquaintance with a person or his personal affairs in his state of seclusion.¹⁸ Accordingly, privacy can only be infringed by the unauthorised acquaintance by an outsider with a person or his personal affairs, which acquaintance can occur in two ways only: first, by intrusion in the private sphere (that is, where an outsider himself becomes acquainted with a person or his personal affairs); and, second, by disclosure or revelation of private facts (that is, where a third party acquaints outsiders with a person of his personal affairs which, although known to that party, remains private).¹⁹ As privacy is closely associated to other personality interests, Neethling has conducted a considerable analysis to distinguish it from such other interests: physical-psychological integrity (including sensory feelings); dignity; identity; autonomy; self-realisation; and patrimonial interests.

Although Neethling's theory of privacy appears to have been postulated in 1976,²⁰ the theory is not novel. Neethling seems to have relied on a similar theory as propounded by Hyman Gross in 1967.²¹ The context in which Gross's conceptualisation of privacy sprang was the US Supreme Court's decision in *Griswold v Connecticut*.²² In this way it may be argued that Neethling's theory of privacy follows the same pattern of Western individualism. Also important, such theory may be classified as falling under the control theory of privacy concept. This notwithstanding, Neethling's theory of privacy has received wider recognition in literature in Africa. Similarly, Neethling's theory has received the approval of the South African Supreme Court of Appeal in *National Media Ltd v Jooste*.²³

17 J Neethling and others *Neethling's law of personality* (1996) 36; J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 19.

18 J Neethling and others *Neethling's law of personality* (2005) 21.

19 As above.

20 J Neethling 'Die reg op privaatheid' ('The right to privacy') LLD thesis, UNISA, 1976.

21 Gross 'The concept of privacy' (1967) 42 *New York University Law Review* 34-54.

22 381 US 479 [1965].

23 1996 (3) SA 262(A) 271.

3 Determinants of privacy concerns in Africa

Privacy concerns, which means a desire to keep personal information to oneself, are essential in determining the adoption of privacy policies and legislation. In Africa such concerns are influenced by various factors. These may broadly be classified as positive or negative determinants. The former relates to factors that operate to cause individuals to be concerned about their privacy and possibly make claim for its protection. It is less important if those factors themselves are positive or negative in their nature but produce one similar result: causing people to be concerned about and value their privacy. The other class of determinants is the negative determinants in the strict sense. The latter constitutes factors operating as impediments to the growth of privacy attitude. Both sets of determinants are considered below. However, before this examination is undertaken it is imperative to consider their nature.

Privacy determinants in Africa characteristically are either spontaneous or non-spontaneous in operation and in producing their effects. Also, some of them are either localised in a particular country or sub-region while others have region-wide influence. Moreover, one or more determinants may operate simultaneously or otherwise in shaping and reshaping privacy attitudes. Important also to point out is the magnitude of these determinants. Quite often the determinants of privacy concerns produce effects at varying degrees: high and low degree. However, this does not suggest undermining the significance of the latter.

One caveat must be read into the above classification of determinants of privacy concerns. The classification presented here undeniably is neither universal, nor is it exhaustive. Yet, it serves to delineate the current major catalysts of privacy concerns in Africa. These may be the bases for policy and legislative developments. Also considering these determinants as not exhaustive leaves it open for future determinants to arise and shape and reshape privacy attitudes in Africa.

3.1 Positive determinants

Development of data banks: Much of the present-day Information and Communication Technology (ICT) in Africa is a result of importation of technology mainly from Europe, the United States and currently from China. While ICT has been an essential tool for information communication, making Africa part of the famous 'global village', it has at the same time posed a number of risks on individuals' personal information. One of the ways in which personal information apparently

is threatened is African governments' tendencies of creating large data banks for various purposes. The latter has manifested mainly in the form of mandatory registration of SIM cards in which all service providers were and are still required as part of their licensing conditions to register all subscribers using their networks. In most cases, the registration of SIM cards in such countries requires subscribers to furnish a wide range of their personal information. The development of SIM card data banks has sparked public debates over the concern over privacy. Part of the reason is the fact that in many countries, such as Tanzania, Kenya, Nigeria, Ghana and Botswana, to mention but few examples, the mandatory registration of SIM cards proceeded, at least initially, on the basis of administrative directives from the national communication authorities in the respective countries.²⁴ There was no legislation or regulation in place for the protection of individuals' personal data.

The other important database in Africa includes those on identification systems (ID systems). Identification systems constitute the most common ICT privacy issue currently facing Africa.²⁵ Such ID systems manifest as national identification cards (national ID cards) leading to the creation of data banks of all nationals in a particular country or passports.²⁶ Both systems use biometric technology. Concerns over privacy here have arisen from the fact that many of the ID systems, such as those in Rwanda and Mozambique, are developed and operated by foreign companies.²⁷ While there is no concrete evidence of any misuse of personal data, these concerns have tended to be insufficiently controlled by African governments in order to prevent such companies from transferring information outside their respective jurisdictions or deal with it in an incompatible manner. As a result, companies may misuse personal information at the peril of individuals. Yet, significant concerns come from security issues as well

24 See, eg, AB Makulilo 'Registration of SIM cards in Tanzania: A critical evaluation of the Electronic and Postal Communications Act, 2010' (2011) 17 *Computer and Telecommunications Law Review* 48; M Murungi 'Registration of mobile phone users: Easier said but carefully done' *Kenya Law* (26 July 2009), <http://kenyalaw.blogspot.com/2009/07/registration-of-mobile-phone-users.html> (accessed 10 November 2021); CE Izuogu 'Data protection and other implications in the ongoing SIM card registration process' (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 10 November 2021); K Anan 'What is my beef against SIM card registration in Ghana?' Independent Civil Advocacy Network, (25 January 2010), <http://www.i-can-ghana.com/?p=104> (accessed 10 November 2021); E Sutherland 'The mandatory registration of SIM cards' (2010) 16 *Computer and Telecommunications Law Review* 61.

25 D Banisar 'Linking ICTs: The right to privacy, freedom of expression and access to information' (2010) 16 *East African Journal of Peace and Human Rights* 126.

26 As above.

27 As above.

as reliability of these databases.²⁸ Rwanda and Kenya (*Huduma Namba* identification system) serve as typical illustrations of misuse of personal information based on ID systems. During the Rwandan genocide of 1994, the national ID cards were used to identify the ‘Tutsi’ victims.

Apart from SIM cards and national ID data banks, in many African countries there are also centralised voter registration databases (CVRDs). The latter in many cases are computerised databases with biometric information, most invariably fingerprints. Privacy concerns with regard to CVRDs have been raised in three main areas. First, most African countries neither have comprehensive data privacy legislation, nor do such countries have legislation or regulations that authorise the collection of voters’ personal information while guaranteeing the protection of privacy.²⁹ Second, where voter registration involves biometrical registration, individuals’ concerns over privacy have been raised high. Third, personal information collected for voting purposes in most cases is shared and re-used for other purposes. This is especially the case in countries where there are no national IDs. In Ghana, apart from voters’ ID cards being used by card holders for private transactions, the same cards have been widely recognised and accepted as official identification by various institutions.³⁰ This is also the case in many other African countries that have not yet adopted national ID card registration systems and sometimes those with national ID systems, such as Tanzania. The privacy issue arising here is that at the time of registration and, hence, the collection of personal data, the respective individuals are not made aware of the disclosure of their personal information to third party institutions or individuals for purposes other than voting. Yet, in defending the practice the electoral commissions, which are the custodians of individuals’ personal data, have always argued that since voters voluntarily use voters’ registration cards for other transactions they have through that given permission for their personal data to be exchanged between those institutions and voters’ roll databases.³¹

Twitter (now X) and Facebook (now Meta) revolutions: The Arab Spring³² in North Africa has demonstrated the clearest instances of violations of

28 As above.

29 A Evrensel ‘Introduction’ in A Evrensel (ed) *Voter registration in Africa: A comparative analysis* (2010) 16.

30 Evrensel (n 29) 16-17.

31 As above.

32 The Arab Spring was a series of anti-government protests, uprisings and armed rebellions that spread across much of the Arab world in the early 2010s. See PK Kumaraswamy ‘The Arab Spring’ (2011) 38 *India International Centre Quarterly* 52

privacy by African governments through the use of modern technologies. First, the Tunisian, Egyptian and Libyan governments used advanced internet filters to block content during the uprisings.³³ In Tunisia the government deployed a far more advanced technology in crackdown through the theft of user names and passwords for Facebook, Twitter and online e-mail accounts such as Gmail and Yahoo!³⁴ This was achieved through the injection of phishing scripts into the content of these pages before being sent to the end user.³⁵ The identification of users was soon followed by arrests, detentions and harassments of those involved in the creation and dissemination of user-generated content.³⁶ Second, Twitter and Facebook were highly used as tools of state surveillance by security and state intelligences to identify and locate activists and protestors.³⁷ Many people participating on Facebook pages were actually government agents or supporters of the regimes, spreading propaganda as well as spying on other Facebook users.³⁸ Third, the regimes, especially those in Egypt and Libya, also demonstrated their ultimate power over the internet by virtually shutting down access to it³⁹ or frequently causing interruptions. The Twitter/Facebook revolutions raised awareness to the majority of Africans over the privacy implications in interacting with social networks and other electronic communications variants. The possibilities to be identified when accessing or exchanging information or opinion, for example, and, above all, the potential possibilities of such communications to be intercepted or monitored with advanced technology have raised more privacy concerns.

Fears: Public fears over threats to privacy and related values have made a significant contribution to the emergence and/or existence of data protection laws, at least in Europe.⁴⁰ One set of such fears related to increasing transparency, disorientation and disempowerment of data subjects in relation to data controllers.⁴¹ Another set of fears concerned the loss of control over technology. A third set pertained to human dehumanisation of societal processes.⁴² In Africa, although it is doubtful

33 Kumaraswamy (n 32) 52.

34 As above.

35 As above.

36 As above.

37 As above.

38 As above.

39 As above.

40 Bygrave (n 5) 107.

41 As above.

42 As above.

whether such fears have had a significant impact in the emergence and/or existence of data protection laws, sufficient fears have been raised regarding privacy encroachments. Two sources of public fears emanate from government surveillance or reprisals and private sector surveillance and unsolicited marketing practices. In the former case, fears for surveillance manifest through the extensive adoption of interception laws by most African governments, including anti-terrorism legislation with interception law provisions.

Surveillance and unsolicited communications for marketing from companies constitute another source of fear over privacy. Alongside these companies' surveillance, individuals also engage in minimum practices of surveillance and by sending unsolicited communications. In either case, the use of closed-circuit television (CCTV) at homes, offices, hotels and large shopping malls is now common in many places in Africa for the purpose of preventing crimes. These technologies are supplemented by SMS text messages. All of these have generated fears for loss of privacy.

HIV/AIDS: Privacy in the context of HIV/AIDS, perhaps, is the most notable area of rising privacy concerns in Africa. HIV/AIDS plagued the African continent in the 1980s. Since then, it has spread significantly. In 2019 there were 20,7 million people with HIV (54 per cent) in Eastern and Southern Africa, 4,9 million (13 per cent) in Western and Central Africa.⁴³ The epidemic had cost the lives of millions of people on the sub-continent. Efforts to prevent or provide care and support to people living with HIV have raised a number of privacy law issues. Consent to HIV testing is the most controversial issue surrounding privacy. Many people in Africa are concerned over HIV testing without their consent. Since there is no prevention of or cure for HIV, many people consider their health records in the context of HIV as most sensitive, fearing stigmatisation.⁴⁴ The second issue stemming from the first concerns the disclosure of HIV test results or status to third parties without authorisation of the persons concerned.

43 HIV Global Statistics, <https://www.hiv.gov/hiv-basics/overview/data-and-trends/global-statistics> (accessed 10 November 2021).

44 See, eg, SD Weiser and others 'Routine HIV testing in Botswana: A population-based study on attitudes, practices, and human rights concerns' (2006) 3 *PLoS Medicine* 1018-1019; NC Mbonu and others 'Stigma of people with HIV/AIDS in sub-Saharan Africa: A literature review' (2009) *Journal of Tropical Medicine* Article ID 145891, 14 pages doi:10.1155/2009/145891; P Anglewicz & J Chintsanya 'Disclosure of HIV status between spouses in rural Malawi' (2011) 23 *AIDS Care: Psychological and Socio-Medical Aspects of AIDS/HIV* 100; The World Bank *Legal aspects of HIV/AIDS: A guide for policy and law reform* (2007), <http://siteresources.worldbank.org/INT/HIVAIDS/Resources/375798-1103037153392/LegalAspectsOfHIVAIDS.pdf> (accessed 10 November 2021).

In response to the above concerns, some governments as well as private sector institutions in Africa such as Ghana, Kenya, South Africa and Tanzania have developed policies as well as special legislation. However, the major weakness of these laws and policies is that they focus on issues of confidentiality alone rather than privacy. Admittedly, while confidentiality is an aspect of privacy, confidentiality as such is inadequate to protect health records in the context of HIV. Apart from that, many of the laws are vague in terms of scope and ambit. Nevertheless, in relative terms concerns for privacy in the context of HIV in Africa has manifested through development of a larger corpus of case law on privacy.⁴⁵ Although such case law still falls short of the principles of data privacy, it serves to demonstrate how far Africans put significant weight on privacy of their health records.

Traumas of past injustices: The concepts of justice and injustice have been a subject of philosophical debates for centuries since the Plato's *Republic*.⁴⁶ Such debates are not covered here because of the little bearing they have on the issues addressed. Yet, it is sufficient to point out that an unjust system presupposes the existence of oppression, exploitation, repression, inhibition or restraints, whether at an individual or group level or by the state. In Africa, the most widely-cited traumas of past injustices are those relating to the system of apartheid in South Africa and the Rwandan genocide.⁴⁷ However, while these are commonly-cited examples of past injustices due to the magnitude of their effects, there are other past injustices in Africa. For example, the dictatorship of military rulers in Africa qualifies for the definition given above. Be that as it may, commentators are in agreement that privacy concerns are nourished by certain concrete experiences, such as the traumas of fascist oppression prior to and during World War II.⁴⁸ Banisar argues that one of the reasons

45 For a detailed review of case law on HIV/AIDS in African jurisdictions, see, eg, MT Ladan 'The role of law in the HIV/AIDS policy: Trend of case law in Nigeria and other jurisdictions' Inaugural lecture delivered at the Ahmadu Bello University, Zaria, Nigeria (2008) 19-22; MA Tadesse 'HIV testing from an African human rights system perspective: An analysis of the legal and policy framework of Botswana, Ethiopia and Uganda' LLM dissertation, University of Pretoria, 2007.

46 See, eg, D Sachs 'A fallacy in Plato's Republic' (1963) 72 *The Philosophical Review* 141-158; J Rawls 'Justice as fairness' (1958) 62 *The Philosophical Review* 164-194; WL McBride 'The concept of justice in Max, Engels, and others' (1975) 85 *Ethics* 204; JA Rawls *A theory of justice* (1971).

47 See, eg, G Weldon 'A comparative study of the construction of memory and identity in the curriculum of post-conflict societies: Rwanda and South Africa' (2003) 3 *International Journal of Historical Learning, Teaching and Research* 55; RU King 'Healing psychological trauma in the midst of truth commissions: The case of Gacaca in post-genocide Rwanda' (2011) 6 *University of Toronto Press Journals* 134-151.

48 Bygrave (n 5) 108.

for adopting privacy laws in many countries, including South Africa, is to remedy privacy violations that occurred under previous regimes and prevent those abuses from recurring.⁴⁹

E-commerce: E-commerce in Africa is still evolving. Its current low level is a result of inadequate e-commerce infrastructure. Yet, where it has started to develop consumer trust and confidence, cyber-crimes and identity thefts have raised serious concerns. This is largely the result of e-commerce transactions collecting vast amounts of personal information. The 'Nigerian Advance Fee Scam' is the most popularly feared across Africa and even beyond, and has caused many privacy concerns in online commercial transactions.

World Summit on the Information Society-Tunis 2005: The World Summit on the Information Society (WSIS) involved a pair of United Nations (UN)-sponsored conferences about information, communication and, in broad terms, the information society that took place in 2003 in Geneva and in 2005 in Tunis. One of its chief aims was to bridge the so-called global digital divide separating rich countries from poor countries by spreading access to the internet in the developing world.⁵⁰ One of the principles of the WSIS in Geneva of 2003 states that '[t]he use of ICTs and content creation should respect human rights and fundamental freedom of others, including personal privacy, conscience, and religion in conformity with relevant international instruments'.⁵¹

Reaffirming the Geneva vision from an African perspective during the WSIS in Tunis (on 16 November 2005), the former President of South Africa, Mr Thabo Mbeki, made the following statement:

Our country and continent are determined to do everything possible to achieve their renewal and development, defeating the twin scourges of poverty and underdevelopment. In this regard, we have fully recognised the critical importance of modern ICTs as a powerful ally we have to mobilise, as reflected both in our national initiatives and the priority programmes of NEPAD, the New Partnership for Africa's Development. We are therefore determined to do everything we can to implement the outcomes of this World

49 D Banisar 'Privacy and data protection around the world' Conference proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999, 2, <http://www.pcpd.org.hk/english/infocentre/conference.html> (accessed 10 November 2021).

50 As above.

51 Geneva Declaration of Principles 2003, Principle 58, Document WSIS-03/GENEVA/DOC/4-E (12 December 2003), <http://www.itu.int/wsisis/docs/geneva/official/dop.html> (accessed 10 November 2021)

Summit on the Information Society and appeal to all stakeholders similarly to commit themselves to take action to translate the shared vision of an inclusive development-oriented information society in practical reality.⁵²

The significance of the WSIS cannot be over-exaggerated. While it did not directly produce its effects over the people, it inspired African governments to commit themselves in using ICT in their development efforts. This also meant that African governments had or have to develop policies and regulations on ICT. To ensure that these commitments are made a reality, WSIS has established a monitoring procedure that periodically conducts follow-up on performance from a country to regional organisation level.⁵³

International, regional and national data protection laws: International, regional as well as national policies and codes for protection of privacy have had impact on privacy in Africa. However, in relative terms, regional policies and codes have been more instrumental in influencing concerns over privacy in Africa and, consequently, the adoption of recent comprehensive data privacy legislation than others. In certain cases, international law offers inspiration for the development of particular domestic legislations or decision-making processes.⁵⁴

At international level, three instruments may be identified that relate to the protection of the right to privacy: the Universal Declaration of Human Rights (Universal Declaration); the International Covenant on Civil and Political Rights (ICCPR); and the UN Guidelines, with regard to the protection of personal data. Since these instruments are UN instrument, they apply to African countries by virtue of their being members of the UN. However, their impact in shaping privacy ideas and consciousness as well as the adoption of policies and regulations has not been significant.

The only regional policy and code of privacy and data protection outside of Africa that has been influential in matters of privacy on the continent was the EU Directive 95/46/EC. It is imperative to mention that the Council of Europe Convention 108 with regard to automatic processing of personal data is the only European regional treaty open for accession by non-European states. Currently, Cape Verde, Mauritius, Morocco, Senegal and Tunisia are the only African states that have acceded to Convention

52 R Capurro 'Information ethics for and from Africa' (2007) 7 *International Review of Information Ethics* 2.

53 See, eg, ITU 'WSIS Forum 2011: Outcome Document' <http://www.itu.int/wsis/implementation/2011/forum/inc/DocumentsWSISForum2011OutcomeDocument.pdf> (accessed 10 November 2021).

54 As above.

108.⁵⁵ Burkina Faso has been invited to accede to the Convention 108 until 24 March 2022.⁵⁶ As has been the case elsewhere, Directive 95/46/EC exerted both political and economic pressure on African countries to adopt data privacy laws in the European style. Article 25 of Directive 95/46/EC provided that the transfer of personal data to third countries would only be allowed if such third countries maintained an adequate level of data protection law similar to the Directive. Yet, since the above European law entered into force in 1998, no African country has been declared as providing an ‘adequate’ level of protection of personal data. In 2010 some African countries that have implemented comprehensive data privacy laws applied to the EU for accreditation as satisfying this level of protection. Included in this list are Mauritius, Burkina Faso, Tunisia, Morocco and Senegal. While the reports for the rest of these countries have not been made public, that of Tunisia is publicly available. As already pointed out, the first report with regard to Tunisia data privacy law made it clear that Tunisia’s regime is not adequate. The rest of the countries had similar outcomes although this was not directly stated in the reports.

In relation to the volume of personal data in the preceding paragraph, the prevailing view is that Africa needs to satisfy the requirements of the European Directive (and now the GDPR) in order to attract investment and outsourcing industries. The economic justification manifests in literature (journal articles, commentaries, reference books, newspapers, magazines and reports), legislation, bills, policies, Hansards, treaties and conventions as well as in *travaux préparatoires*. It is worth noting that the economic justification behind the adoption of data privacy legislation in Africa has also manifested in the reports for analysis of the adequacy of protection of personal data in some African countries.⁵⁷ Similarly, the justification was prominent in parliamentary discussions in Mauritian, Kenyan and in the South African legislative process.⁵⁸ As pointed out, there currently

55 Council of Europe ‘Chart of signatures and ratifications of Treaty 108’, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=jESnZmay (accessed 10 November 2021).

56 Council of Europe ‘Non-member states of the Council of Europe: Five years validity of an invitation to sign and ratify or to accede to the Council of Europe’s treaties’, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22> (accessed 10 November 2021).

57 See, eg, CRID (Centre de Recherches Informatique et Droit), University of Namur (Belgium) ‘Analysis of the adequacy of protection of personal data provided in Tunisia-Final Report’ (2010) 7, http://alexandrie.droit.fundp.ac.be/GEIDFile/6544.pdf?Archive=192619191089&File=6544_pdf (accessed 10 November 2021).

58 PMG., ‘Protection of Personal Information Bill [B9-2009] briefing’, 7th October 2009; <http://www.pmg.org.za/report/20091007-protection-personal-information-bill-b9-2009-briefing> (accessed 10 November 2021).; Portfolio Committee on Justice

is no general survey to concretise the extent to which African countries have economically been affected by the restriction on the transfer of personal data from Europe. In most cases, such claims have been made by sweeping statements. However, on country level, Morocco seems to have undertaken a study on the impacts of European data privacy law. In 2008 a report by the Moroccan Ministry of Economy pointed out that the low volume of relocation of banking and insurance services to Morocco was partly due to a lack of protection of personal data transferred to the kingdom, and recommended the adoption of legislation of this subject, which followed in 2009.⁵⁹

3.2 Negative determinants

Lack of awareness of privacy risks: Privacy awareness reflects the extent to which an individual is informed about privacy practices and policies, about how disclosed information is used, and being cognisant about their impact over the individual's ability to preserve his private space.⁶⁰ A lack of privacy awareness perhaps is one of the most negative determinants that have impeded the growth of privacy concerns in Africa and, consequently, affecting the adoption of privacy policies and legislation. Understandably, this lack of individuals' awareness of privacy risks partly reflects the value Africans attach to privacy of their personal information. Sometimes privacy policies and legislation may exist in African countries, but ignorance by individuals produces the same result. Extending the concept of the 'privacy myopia' in the African context while explaining the value attached on privacy by individuals in Uganda, Bakibiknga argues that Ugandans largely suffer from 'privacy myopia'.⁶¹ This also is the case in other African countries such as Nigeria, as explained by Kusamotu.⁶² Yet,

and Constitutional Development., 'Background Information: Protection of Personal Information Bill [B9-2009], Deliberations 4th November 2009; <http://www.pmg.org.za/report/20091104-protection-personal-information-bill-b9-2009-deliberations> (accessed 10 November 2021).; Mauritius National Assembly, Debate No 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004); Parliament of Kenya, The National Assembly, 'Hansard Report', Wednesday 6 November 2019.

59 Ministère de l'Economie et des Finances, *Dé localisation des activités de services au Maroc, Etat des lieux et opportunités* (Juillet 2008) 15, http://www.finances.gov.ma/depf/publications/en_catalogue/etudes/2008/delocalisation.pdf (accessed 10 November 2021).

60 H Xu and others 'Examining the formation of individual's privacy concerns: Toward an integrative view' *International Conference on Information Systems (ICIS) Proceedings* (2008) 6.

61 Bakibinga (n 15).

62 A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46' (2007) 16 *Information and Communications Technology Law* 157.

a lack of awareness of privacy risks should not be regarded as a natural phenomenon. There are a range of factors that offer an explanation for this situation. This includes a low level of computerisation or penetration of technology in Africa, resulting in the corresponding low level of data processing and awareness about its implications for privacy.⁶³ This penetration level has resulted into the 'digital divide' between urban and rural Africa.

A survey⁶⁴ by Ipsos has found that, compared to those living in developed nations, people in countries with lower economic living standards (Nigeria, Kenya and Tunisia) tend to have lower online privacy concerns with regard to personal information being monitored or bought and sold. Such individuals are also relatively less concerned about a general lack of privacy due to having so much information about themselves on the web. The survey further found that although over the past few years, developing nations have experienced some fast growth in the number of new internet users and smartphone owners, leading to exponentially sharper increases in the number of people who are newly exposed to online social networking, business transaction and e-commerce compared to nations with higher GDP per capita, privacy concerns have remained relatively low. The survey shows that increased familiarity with online experiences may not necessarily imply greater awareness of privacy issues or the ability to protect one's personal information. This is because most developing nations still have a nascent or poorly implemented institutional frameworks around data privacy. These findings are consistent with more recent surveys which have established that although Kenya, South Africa, Togo and Uganda have comprehensive data protection legislation, this is not necessarily a strong indicator of commitment to protection of privacy rights, or of efficacy of the legislative environment in ensuring the right to privacy and data protection.⁶⁵ Reports across these countries already indicate that an asymmetry between legislation and practice is evident at different levels. This is confirmed by a survey conducted by WorldWideWorx and commissioned by global technology company Zoho, which finds that 78% of South African businesses are unaware of privacy laws governing their marketing activities.⁶⁶

63 As above.

64 EH Rho and others 'Differences in online privacy and security based on economic living standards: a global survey of 24 countries', Research Paper, Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018 at 11.

65 A Finlay 'Introduction and Overview' in *African Declaration on Internet Rights and Freedoms Coalition*, *Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries* <https://africaninternetrights.org>, May 2021, pp. 5-14.

66 Creamer Media Reporter (ed)., '78% of South African businesses are unaware about

Another factor affecting awareness is the high level of illiteracy in Africa.⁶⁷ With this general low illiteracy level, individuals' ability to understand threats posed upon their privacy becomes severely limited. However, this does not suggest that literate individuals are well placed to understand privacy risks to their personal information. A survey conducted across Africa, 'Awareness Survey on Freedom of Information and Data Protection Legislation and Open Government Data Initiatives'⁶⁸ from 27 to 30 September 2011 provides solid evidence that a lack of awareness of privacy risks affects a large number of literate individuals working in private sectors, governments, academic and researcher institutions.

Apart from the above factors affecting awareness, it is difficult to entirely disagree that African culture impacts on an individual's awareness and consciousness of privacy, particularly in rural areas where a collectivist life style is still discernible. As pointed out by some commentators, through group association in African cultures, an individual's interests are subordinate to those of groups. Accordingly, there is sharing of even sensitive personal information with others without being aware of the likely resulting privacy risks. Yet, while collectivist culture operates as a negative determinant, there has been rare discussion, let alone mention, of culture in the legislative processes and the *travaux préparatoires* to the data privacy laws leading to data protection legislation in Africa. This may partly be due to two main factors: over-dominance of economic justifications for adopting such legislation as state-sponsored agenda as well as its attendant propaganda and lack or inadequate public consultation during the legislative processes around data privacy laws.

Resistance to transparency: Some governments resist taking an interest in privacy issues as they do not wish to become more and more transparent and accountable to their citizens. The resistance may be demonstrated generally by the rejection of the bills of rights in the independent constitutions or restricting its application; the rejection of access of information legislation or the restriction of their application; and, specifically, being indifferent

privacy laws governing their marketing activities, rely heavily on third-party trackers and ad platforms – Survey' <https://www.engineeringnews.co.za/article/78-of-south-african-businesses-are-unaware-about-privacy-laws-governing-their-marketing-activities-rely-heavily-on-third-party-trackers-and-ad-platforms-survey-2021-06-21>

67 See, eg, UNESCO Institute for Statistics 'Adult and youth literacy' Fact Sheet (September 2011), <http://www.uis.unesco.org/FactSheets/Documents/FS16-2011-Literacy-EN.pdf> (accessed 10 November 2021).

68 K Taylor 'Awareness survey on freedom of information and data protection legislation and open government data initiatives' The Internet Governance Forum, Nairobi, Kenya, 27-30 September 2011 1-19, http://epsiplatform.eu/sites/default/files/IGF6_W123_PSI_Surveyreport_21October2011.pdf (accessed 10 November 2021).

in initiating the legislative process for data protection legislation, which in some ways places governments under certain obligations in processing personal information. This in turn limits the ability of governments to conduct unregulated surveillance over their people.

Lack of or inadequate legislative consultation: Historically, the drafting and enactment of data protection laws around the world, particularly in Europe, have frequently been lengthy processes fraught with controversy.⁶⁹ Yet, in some places, such as Sweden, the preparation and enactment of data protection legislation occurred relatively quickly and smoothly.⁷⁰ However, this does not suggest that data privacy legislation in Sweden was adopted without public consultation or in only few days. In Africa, with the exception of a few countries (such as South Africa and Kenya), the enactment of data privacy legislation had not engaged public consultation or such consultation had been inadequate. Ordinarily, public consultations in the legislative process generate debates about the necessity or otherwise of data privacy laws, their contents, enforcement, and so forth, which stimulates interest in and awareness about these laws to the public. Concomitantly, they facilitate the implementation of data privacy laws once enacted.

Cost: The costs of adopting and implementing comprehensive data protection legislation are also among critical issues for developing countries. Such costs are borne with respect to carrying out training, awareness-raising programmes, seminars, the conducting of investigations, dispute resolution, and so forth. As most African governments' annual budgets depend to over 30 per cent of budget support from donors,⁷¹ it practically is difficult to finance the adoption and implementation of data privacy legislation.

4 Policy and regulatory frameworks for privacy and data protection

Policy and regulation of privacy and personal data protection in Africa can be considered at regional, sub-regional and national levels. At the regional level, various instruments have been developed under the auspices of the African Union (AU). Under sub-regional level there are initiatives by Economic Community of West African States (ECOWAS); the East

69 Bygrave (n 5) 4.

70 Bygrave (n 5) 5.

71 M Knoll 'Budget support: A reformed approach or old wine in new skins?' UNCTAD Discussion Papers 190 (October 2008) http://www.unctad.org/en/docs/osgdp20085_en.pdf (accessed 10 November 2021).

African Community (EAC); and the Southern African Development Community (SADC). Fewer initiatives are known to have taken place in the Common Market for Eastern and Southern Africa (COMESA) and Economic Community of Central African States (ECCAS), and Arab Maghreb Union (UMA).

4.1 The African Union

4.1.1 Human rights treaties

The African Charter on Human and Peoples' Rights (African Charter) is the main human rights treaty of the AU.⁷² One of the objectives of the AU is to promote international cooperation having due regard to the Charter of the UN and the Universal Declaration.⁷³ This objective partly necessitated the adoption of the African Charter in 1981 in Africa. Concomitantly, the African Charter incorporates universal human rights standards and principles similar to those in the Universal Declaration. However, in contrast to the Universal Declaration, the African Charter has its unique elements that reflect the virtues, culture and values of African traditions. First, the African Charter creates a reciprocal relationship between the individual and the community, linking individual and collective rights. Second, the African Charter creates a set of obligations that have to be fulfilled by an individual in order to enjoy the rights established.

As far as the protection of the right to privacy is concerned, the African Charter contains no express provision. This omission has erroneously led many commentators to conclude that Africans do not value privacy.⁷⁴ However, some commentators have advanced the argument that despite such an omission, privacy may still be read into other provisions, particularly the right to dignity.⁷⁵ Although this argument makes sense, neither the African Commission on Human and Peoples' Rights (African Commission) nor the African Court on Human and Peoples' Rights (African Court), the main mechanisms under the African Charter, has so far provided an authoritative interpretation to that effect. This is despite the fact that the African Court has jurisdiction over all cases and disputes

72 OAU African Charter on Human and Peoples' Rights OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), 27 June 1981, entered into force 21 October 1986 (African Charter).

73 OAU Charter 1963, art II(1).

74 See, eg, Gutwirth (n 11); Bygrave (n 12).

75 AB Enyew 'Regulatory legal regime on the protection of privacy and personal information in Ethiopia' LLM dissertation, University of Oslo, Norway, 2009 15, <https://www.duo.uio.no/bitstream/handle/10852/22947/Binder1%5B1%5D.pdf?sequence=1&isAllowed=y> (10 November 2021).

submitted to it concerning the interpretation and application of the African Charter, the African Court Protocol, and any other relevant human rights instrument ratified by the states concerned.⁷⁶

There are limitations to the realisation of the rights stipulated under the African Charter generally through the available mechanisms. This is due to the fact that, although the African Commission has the power to receive complaints from individuals, its decisions are non-binding on a state party and, above all, they are considered confidential until they are approved for publication by the Assembly of Heads of State and Governments.⁷⁷ This is one of the reasons why the African Court was established. Interestingly, the African Court Protocol does not grant individuals direct access to the Court, as is the case with states and organisations. In this case, the African Court has a discretion to allow or disallow an individual to file a case.⁷⁸ Moreover, an individual cannot merely file a case to the Court if the relevant state has not made a declaration during the ratification of the Protocol, of accepting the jurisdiction of the Court to hear and determine such a case.⁷⁹

The African Charter on the Rights and Welfare of the Child (African Children's Charter) is the only AU instrument that expressly guarantees the right to privacy. Article 10 of the Children's Charter states:

No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.

The adoption of the African Children's Charter defeats the popular argument that the omission of a provision for protection of privacy in the African Charter is sufficient evidence to support the claim that Africans do not value privacy. However, one point must be clearly made, namely, that the main influence for the adoption of the African Children's Charter is the UN Convention on the Rights of the Child of 1989.⁸⁰ The right to privacy is one of the provisions in the UN Convention. Yet, it still is not

76 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, 2004 art.3 (African Court Protocol).

77 Art 59(1) African Charter.

78 Art 5(3) African Court Protocol.

79 Art 34(6) African Court Protocol.

80 United Nations Convention on the Rights of the Child 1989; adopted 20 November 1989 and entered into force 2 September 1990.

clear why the African Charter omits a clause on the protection of privacy despite the fact that it makes reference in its Preamble to the Universal Declaration and ICCPR that contain clear provisions on the protection of the right to privacy. The provisions on the rights to privacy in the Universal Declaration and ICCPR directly apply in some African countries of which the treaty practice is monism. Moreover, in dualist African states these provisions have also permeated into national constitutions after incorporation processes.

4.1.2 The African Union Convention

The AU Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention) is the continental binding treaty in the field of cybersecurity. The Convention was adopted by the twenty-third ordinary session of the Assembly, held in Malabo, Equatorial Guinea, on 27 June 2014. It just recently entered into force having obtained the fifteen ratifications required by its article 36.

The history of the Malabo Convention dates back to the Addis Ababa Declaration by the Heads of State and Government of the AU on 2 February 2010.⁸¹ In this Declaration it was alluded to the fact that information and communication technologies (ICTs) are powerful catalysts for the development and integration process in Africa. However, it was realised that ICTs need to be regulated. Because of this, the establishment of a legal and regulatory framework that is harmonised and attractive to investments, shared telecommunications and ICT infrastructure as well as the convergence of networks, services and administration became necessary. In the context of the Addis Ababa Declaration, the Malabo Convention was adopted.

The Malabo Convention regulates three sets of issues: electronic transactions (chapter I); personal data protection (chapter II); and cybersecurity/cybercrimes (part III). Of interest in this part is the protection of personal data. One point has to be made clear from the outset. The Malabo Convention has been significantly influenced by the European data protection regimes, namely, the European Union Data

81 AU Addis Ababa Declaration on Information and Communication Technologies in Africa: Challenges and prospects for development, Assembly/AU/Decl.1(XIV), adopted by the 14th ordinary session of the Assembly in Addis Ababa, Ethiopia on 2 February 2010.

Protection Directive 95/46/EC, the Council of Europe Convention 108 and the OECD Guidelines.⁸²

As far as the protection of personal data is concerned, the Malabo Convention requires each member of the AU to put in place a legal framework with a view to strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punishing any violation of privacy without prejudice to the principle of the free flow of data.⁸³ Further, such mechanism must ensure that any processing of personal data respects the freedom and fundamental rights of natural persons while at the same time recognising the prerogatives of the state, the rights of local communities and the purposes for which businesses were established.⁸⁴

The scope and application of the Malabo Convention are too broad.⁸⁵ It applies to data processing undertaken by private and public sectors. In both cases the Convention extends its application to processing of personal information of natural person and legal entities. Moreover, the Malabo Convention targets both automated and non-automated processing of personal data. The territorial application of the national data privacy is restricted to the processing of data taking place in the territory of a member state. Processing operations concerning public security, defence, state security and criminal law are also within the scope and application of the Convention. However, the Convention gives member states leverage to make exceptions under specific provisions of national legislation. Since the scope of these leverages is not clear, in practice a state may entirely exclude the application of the Convention on such types of data processing.

The Malabo Convention does not apply where processing takes place within the exclusive context of personal or domestic activity and where temporary copies are produced in the context of technical activities for transmission and access to a digital network for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted.⁸⁶ While the first exception in the Convention is similar to European data protection regimes, the former is further qualified, in that such data processing is not meant to be carried out for systematic

82 For a critical appraisal of the Malabo Convention, see generally LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

83 Art 8(1) Malabo Convention.

84 Art 8(2) Malabo Convention.

85 Art 9(1) Malabo Convention.

86 Art 9(2) Malabo Convention.

communication to third parties or for further dissemination. Practically, this additional qualification serves no value as any processing concealed to be undertaken under the cover of personal or domestic activities and subsequently discovered to be inconsistent with such purposes and limits will automatically be taken to fall short of this exception.

The Malabo Convention contains six data processing principles similar to EU data protection regimes.⁸⁷ The first principle is consent to and legitimacy of personal data processing. This principle does not apply in specific cases enumerated by the Convention. The second principle is the principle of lawfulness and fairness of personal data processing. The third is the principle of purpose, relevance and storage of processed personal data. Repurposing against the original purpose is restricted. The fourth principle is the principle of accuracy of personal data. The fifth principle is transparency of personal data processing. The sixth principle is confidentiality and security of personal data processing. The Convention also contains provisions on the protection of sensitive data.⁸⁸

As it is conventional to most data protection regimes, the Malabo Convention contains rights of data subjects: the rights to information, access, object and rectification or erasure.⁸⁹ It also sets out obligations on data controllers. These include confidentiality, security, storage and sustainability obligations.⁹⁰

Similarly, the Malabo Convention contains rules on transborder data movement. Article 14(6) of the Convention states that a data controller shall not transfer personal data to a non-member state of the AU unless such state ensures an adequate level of protection of privacy, freedoms and fundamental rights of persons whose data are being or likely to be processed. Surprisingly, the Convention neither provides criteria for assessing the level of adequacy of data protection, nor does it expressly indicate who is to undertake such assessment, although, this should be the national data protection authority. Institutionally, the Malabo Convention obliges every member of the AU to establish an authority with responsibility to protect personal data.⁹¹

87 Art 13 Malabo Convention.

88 Art 14 Malabo Convention.

89 Arts 16-19 Malabo Convention.

90 Arts 20-23 Malabo Convention.

91 Art 12(1) Malabo Convention.

4.2 Sub-regional frameworks

4.2.1 *ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection*

The Economic Community for West African States (ECOWAS) has 15 members.⁹² ECOWAS was established by the Treaty of Lagos on 28 May 1975 with the objective of promoting cooperation and economic integration in the West African region through the harmonisation of policies and laws.⁹³

In terms of data privacy protection, ECOWAS is the first and only sub-regional grouping in Africa to develop a concrete framework of data privacy law, namely, the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. The Act has been strongly influenced by the EU Directive. In turn, the Supplementary Act has strongly influenced the Malabo Convention. The latter in fact has replicated the former word-to-word with only a few exceptions. Because of this, the analysis with regard to the Supplementary Act is unnecessary and the comments made above regarding the Malabo Convention apply.

It also is worth noting that contrary to the Malabo Convention, the Supplementary Act is an integral part of the ECOWAS Treaty.⁹⁴ Breaches of the Supplementary Act by member states can be enforced before the ECOWAS Court of Justice.

4.2.2 *EAC Legal Framework for Cyber Laws 2008/2011*

The East African Community (EAC) comprises six countries: Kenya, Uganda, Tanzania, Rwanda, Burundi and South Sudan. The Community was established in 1999 by the Treaty for Establishing of the East African Community 1999. The major aim of the EAC is to foster development among the member states. To this end, the EAC established a Customs Union in 2005 and a Common Market in 2010.

The EAC has not been isolated by the development of ICTs. The potential benefits and risks of using ICTs are issues that recently have gained prominent discussion in the EAC. In this regard, the realisation of a solid cyber law in the Community is essential in underpinning the

92 Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

93 Art 3 ECOWAS Treaty 1975.

94 Art 48 ECOWAS Supplementary Act 2010.

implementation of the Common Market Protocol, especially regarding services, an area of great potential for the region.⁹⁵ However, the sub-region as yet does not have a legal framework for the protection of personal data. Currently, only Kenya and Uganda have adopted comprehensive data protection legislation.

4.2.3 SADC Model Law on Data Protection 2012

The Southern African Development Community (SADC) is a sub-regional grouping of 15 countries: Angola, Botswana, the Democratic Republic of the Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. It was formed in Lusaka, Zambia, on 1 April 1980, following the adoption of the Lusaka Declaration. The main objectives of the SADC are to foster economic, political and social development in the member states.

As far as privacy and data protection is concerned, the SADC has adopted a model law on data protection in the sub-region, namely, the SADC Model Law on Data Protection 2012 (Model Law). The Model Law is heavily influenced by the European Directive 95/46/EC. However, there are significant differences in scope and ambit for the principles covered in these sets of laws. These are not considered here. It is important to note that the Model Law is not a binding instrument and, as such, it has little influence on law reforms in the sub-region.

4.3 National constitutions and data protection legislation

There are two main frameworks of protection of data privacy at national level in Africa: constitutions and statutory laws. The highest order of such protection is the national constitution of a respective country. In this category there are countries with express provisions for the protection of privacy in their constitutions.⁹⁶ This presents the largest group. The second group includes countries of which the constitutions lack express provisions on the constitutional right to privacy. For example, article 20 of the Angolan Constitution 2010 refers to the protection of personal integrity, the good name and reputation. It is silent on privacy protection. The third group has constitutions that maintain two sets of provisions for

95 Dr Enos Bukuku, the EAC Deputy Secretary-General in charge of Planning and Infrastructure; see UNCTAD 'Press clipping: EAC develops cyber laws' (25 October 2011) http://r0.unctad.org/ecommerce/docs/EAC_Media.pdf (accessed 10 November 2021).

96 See, eg, Tanzania, Kenya, Nigeria, Mauritius, South Africa and Botswana.

the protection of privacy or personality right. The first set relates to the express provision of a constitutional right to privacy while, the second set is *habeas data*.⁹⁷

As a basis for protecting privacy, a constitution has three limitations. First, the scope of the constitutional right to privacy depends on courts' interpretation on a case-to-case basis. This renders the law uncertain until the actual case has been filed in court. Currently this case law is scant (South Africa, Kenya, Uganda, Tanzania, Mauritius) or lacking in some jurisdictions. Second, in most cases constitutions only protect against infringements of privacy committed by the state and its agencies. The private sector is excluded. Since the private sector is fast growing and expanding in Africa, constitutional protection does not prevent the misuse of personal information by businesses and private sector entities. Third, infringements of the constitutional right to privacy attract different remedies from those obtained under data protection legislation. For example, monetary compensation is not a remedy under breaches of constitutional provisions.

Apart from constitutional protection, there are also statutory protections. These are either by comprehensive data protection legislation, sectoral laws or *ad hoc* provisions in different statutes. Currently there are 30 African countries with comprehensive data protection legislation.⁹⁸ With the exception of the recently-adopted data protection legislation, which is based on the European General Data Protection Regulation, the rest of the data protection laws are based on the now-repealed European Union Data Protection Directive 95/46/EC. The main manifestations of sectoral law protecting privacy are those in the communications sector, health and employment. However, in most cases these sectoral laws fail to address specific principles in the relevant sector. This is the case, for example, in the employment sector and the requirements of the mandatory or concealed pre-employment HIV test by employers. In case of *ad hoc* provisions, the laws contain only few sections that may have a privacy implication.

There finally is protection of privacy through the common law. This form of privacy protection is clearly available in a few African countries (for instance, South Africa). South Africa currently is the only African

97 See, eg, Cape Verde and Angola.

98 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Congo-Brazzaville, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea Conakry, Côte d'Ivoire, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, São Tomé and Príncipe, Senegal, Seychelles, South Africa, Togo, Tunisia, Uganda.

jurisdiction that has a relatively large corpus of case law on common law privacy. However, such case law does not offer prescriptive guidance in terms of the scope and ambit of principles.

5 Analysis of data privacy policies in Africa: Patterns and trends

As pointed out, 30 out of 55 African countries have adopted data protection legislation. Cape Verde is the first African country to enact data protection legislation in 2001. The latest country to adopt data protection legislation is Egypt (July 2020). The following is the analysis of the major trends/patterns of the African data privacy legislation and practice:

- *Inspired by EU-data protection governance*

Data privacy laws in Africa (national, regional and continental) are largely inspired by the EU data protection regime, mainly the now-repealed Data Protection Directive 95/46/EC. Articles 25-26 of this Directive comprised the restriction of data export outside EU to third countries without an ‘adequate level’ of protection. Since the rest of the world, including Africa, has trade relations with EU countries, the ‘adequacy requirement exerted indirect pressure on African countries to enact data protection legislation based on the EU style.

With the repeal of the Data Protection Directive and its replacement by the GDPR, some African countries have revised their laws to match up with the GDPR standards (for instance, Mauritius). However, countries that adopted data protection after the GDPR has been in force have attempted to enact such laws in compliance with the GDPR (for instance, Uganda, Kenya, Egypt). It is worth noting that, although South Africa adopted its data protection legislation (POPIA) in 2013, almost five years before the GDPR entered into force, it took into consideration provisions of the early texts of the GDPR. Hence, it is mostly based on the GDPR.

It is noticeable that EU through its institutions, CoE, the United Nations Conference on Trade and Development (UNCTAD), and ITU through various programmes offered technical support to Africa to assist African governments to put in place data protection legal frameworks. This means that there still is limited capacity in Africa to adopt data privacy laws. Yet, this questions how issues of context are handled in law reform processes.

- *Little influence of African constitutions, continental and regional privacy policies*

Most objective clauses of data protection bills/laws in African countries stipulate that one of the reasons for adopting data privacy legislation is 'to give effect to a constitutional provision on the right to privacy'. However, the value of the constitutional right to privacy is questionable. It certainly is known that at independence in the 1960s and 1970s, many African countries adopted constitutions with a bill of rights that included an express provision on the right to privacy. However, for more than 40 years such provisions on the right to privacy have never been implemented by legislation, nor have such provisions been litigated upon to result in strong privacy jurisprudence except on a very limited scale (for instance, in South Africa, Kenya, Nigeria, Uganda and Tanzania).

Likewise, Africa has put in place binding data privacy treaties/agreements such as the African Union Convention on Cyber Security and Personal Data Protection 2014 and the ECOWAS Supplementary Act on Personal Data Protection 2010. There are also non-binding instruments (soft law) such as SADC Model Law on Data Protection 2012; the EAC Framework for Cyberlaw I, 2010; the ECCAS Model Law on Data Protection 2013; and the AU/Internet Society Personal Data Protection Guidelines for Africa 2018.

Overall, the above instruments have similar provisions with slight wording. They have also been influenced by the European data protection regimes. As pointed out, AU and ECOWAS instruments are the only binding agreements, while the rest constitute soft law. The issue is to what extent African regional and continental instruments have been influential to the data privacy law reform in Africa. It is difficult to see any such influence. The AU Convention was adopted in 2014. So far it has not entered into force for want of 15 ratifications. Five years have now lapsed since the Convention was adopted without it entering into force. Which influence then could it provide? Inspirational or what? Assuming that the Convention had already been in force, it lacks equivalent institutions such as those in the GDPR/EC Directive 95/46/EC which could monitor compliance. This also is the limitation with respect to the ECOWAS Supplementary Act on Personal Data Protection. Moreover, the preparatory documents of data privacy law in African countries indicate no reference to the African continental and regional privacy policies. Instead, express reference and detailed discussion is made to the European privacy regime by then EC Directive 95/46/EC (repealed) and now the GDPR. Moreover, in 2010 four African countries (Burkina Faso, Mauritius, Tunisia and Morocco) attempted to seek accreditation of

their data protection systems to the EU.⁹⁹ As pointed out, a preliminary assessment indicated that they all fell below the EU adequacy standards. Renewed efforts by these states and others in Africa to race to Europe are now being made through accession to the CoE Convention 108 as an alternative route, which appears to be less stringent to comply.¹⁰⁰

- *Flawed law reform process*

It is interesting to note that with the exception of a few countries, data protection and law reform in Africa has largely been an exercise of copy and paste of European law.¹⁰¹ This is attributed to a number of reasons: a lack of competent experts in the area of data privacy law; a lack of interest and avoidance of cost by governments to invest in the reform process; attempts to show to Europe that national legislation are strictly according to the Directive 95/46/EC or GDPR, hence facilitating accreditation of such legislation, and so forth. Concomitantly, in many African countries privacy law reform is simply about legal drafting and nothing more. There normally is a lack of and/or limited debates and public consultation. The second EU consultant notes that ‘much of the existing legislation (in Mauritius) was copied from much larger countries, notably United Kingdom, New Zealand and South Africa, without a thorough analysis of the actual needs and capacities of Mauritius, and without much learning from the experiences of other small island developing states’.¹⁰² While borrowing and legal transplantation are acceptable and perhaps are inevitable in the field of data privacy law, the domestication of European law into the African context is not only important but necessary. Greenleaf correctly observes that ‘most striking, the African regional framework (as well as national legislation) does not display any African-specific approach to data protection’.¹⁰³ However, attempts to domesticate such laws must be done with caution. The Nigerian and Kenyan (first drafts) data privacy

99 AB Makulilo ‘Data protection regimes in Africa: Too far from European “adequacy” standard?’ (2013) 3 *International Data Privacy Law* 42-50.

100 AB Makulilo ‘African accession to Council of Europe Privacy Convention 108: Moving towards stronger privacy protection’ (2017) 41 *Datenschutz und Datensicherheit-DuD* 364-367.

101 AB Makulilo ‘Data protection and law reform in Africa: A systematic or flawed process?’ (2016) 2 *International Journal of Technology Policy and Law* 228-241.

102 Confidential report ‘Ensuring the compliance of the data protection legislation and principles of Mauritius with EU standards, 2011’ 4.

103 G Greenleaf & B Cottier ‘Comparing African data privacy laws: International, African and regional commitments’ University of New South Wales Law Research Series (2020) 33, <https://ssrn.com/abstract=3582478> or <http://dx.doi.org/10.2139/ssrn.3582478> (accessed 10 November 2021).

Bills demonstrate poor examples as they contain limited provisions with regard to processing personal data.¹⁰⁴

- *Lack of international harmonisation*

As data-processing operations increasingly extend across national boundaries, the way in which they are to be regulated should take account of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation.¹⁰⁵ With respect to Africa, Makulilo has extensively discussed the challenges of harmonisation of data privacy policies.¹⁰⁶ Chiefly among these is the existence of multiplicities of regional privacy policies. Even though such policies contain similar provisions, it is difficult for them to drive Africa towards a common point. As pointed out, most of the instruments are non-binding while only the ECOWAS Supplementary Act and AU Convention are binding. Similarly, it has been pointed out that the AU Convention has not yet entered into force. The other reason is the lack of centralised institutions to monitor compliance with the policies, especially the AU Convention. There also is the question of existing different legal systems among the participating countries in regional economic communities (RECs) and at the AU level, which has led to somewhat divergent legislative practices and procedures between the groups of countries. These legal systems are largely made up of the common and civil law legal systems.

- *Lack of and/or weak enforcement*

This is one of the aspects that raises many questions about the value of data privacy in Africa. So far 12 out of 30 African countries with data privacy legislation have not yet appointed data protection authorities.¹⁰⁷ While there is no particular standard time for a data protection authority to be appointed, six out of the 12 African countries have so far continued

104 AB Makulilo 'Nigeria's Data Protection Bill: Too many surprises' Privacy Laws and Business International Report, 2012, No 120 25-27; Article 19 'Nigeria: Personal Information and Data Protection Bill', <http://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill> (accessed 10 November 2021). Article 19 'Kenya: Draft Data Protection Bill critically limited', <http://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited> (accessed 10 November 2021).

105 Bygrave (n 5) 12.

106 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer, Law and Security Review* 78-89.

107 Algeria, Botswana, Chad, Congo Brazzaville, Egypt, Equatorial Guinea, Guinea Conakry, Madagascar, Mauritania, Niger, Seychelles, Togo.

for one to four years without a data protection authority in place.¹⁰⁸ One may argue that this is still a reasonable time. However, the other six African countries have taken a minimum of five to a maximum of 16 years without appointing a data protection authority.¹⁰⁹ Cape Verde, the first African country to adopt data protection legislation in 2001, only appointed a data protection authority in 2017, after 16 years. Seychelles, the second African country to adopt data protection legislation, has to date not brought its law into force. South Africa, which passed its data protection legislation in 2013, has only brought the substantive part of the law in force in 2020, almost seven years later.

It is also important to note that the majority of countries with appointed data protection authorities have not done much as far as enforcement is concerned. In 2012, 2014 and 2020 Makulilo closely analysed the enforcement of the data protection legislation in Mauritius based on the repealed law (2004) and the new legislation (2017). He came to the conclusion that although Mauritius is doing well regarding enforcement, a number of shortcomings have to be addressed. One of the issues about which the data protection authority is complaining is inadequate resources (both financial and human) to support the activities and functions of the authority. In the beginning, the interpretation of the law based on complaints referred to the data protection authority was not consistent in similar complaints and at times other considerations outside the data protection legislation were taken into account. However, under the new data protection legislation there is consistency in the interpretation of similar complaints.

6 Conclusion

This chapter has illustrated that after a lapse of two decades, significant developments have taken place in Africa as far as data protection is concerned. First and foremost, there has been a steady increase and interest of many African governments to adopt data privacy policies and laws. Second, there have been attempts to harmonise data privacy laws and policies across Africa through the adoption of a continental treaty on data privacy as well as sub-regional levels. Also, important to note, African governments have gained interest to accredit their data protection systems to the most advanced, particularly those in Europe, in order to facilitate free flow of personal information. This in turn may boost African economies through foreign investment. However, the growth and development of data privacy in Africa still faces critical challenges, as discussed above.

108 Algeria, Botswana, Congo Brazzaville, Egypt, Niger, Togo.

109 Cape Verde, Chad, Guinea Conakry, Madagascar, Mauritania, Seychelles.

Nonetheless, there are still prospects for African governments to address such challenges through international cooperation.

References

- Abdulrauf, LA & Fombad, CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67
- Anan, K 'What is my beef against SIM card registration in Ghana? Independent Civil Advocacy Network (25 January 2010), <http://www.i-can-ghana.com/?p=104> (accessed 10 November 2021)
- Anglicewicz, P & Chintsanya, J 'Disclosure of HIV status between spouses in rural Malawi' (2011) 23 *AIDS Care: Psychological and Socio-Medical Aspects of AIDS/HIV* 998
- Bakibinga, EM 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective' (2004) <http://thepublicvoic.org/eventscapetown04/bakibinga.doc> (accessed 10 November 2021)
- Banisar, D 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 *East African Journal of Peace and Human Rights* 124
- Banisar, D 'Privacy and data protection around the world' Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999 1, <http://www.pcpd.org.hk/english/infocentre/conference.html> (accessed 10 November 2021)
- Bennett, CJ *Regulating privacy: Data protection and public policy in Europe and the United States* (Cornell University Press 1992)
- Bygrave, LA *Data protection law: Approaching its rationale, logic and limits* (Kluwer Law International (2002)
- Bygrave, LA 'Privacy protection in a global context: A comparative overview' (2004) 47 *Scandinavian Studies in Law* 319
- Bygrave, LA *Data privacy law: An international perspective* (Oxford 2014)
- Capurro, R 'Information ethics for and from Africa' (2007) 7 *International Review of Information Ethics* 1
- Enyew, AB 'Regulatory legal regime on the protection of privacy and personal information in Ethiopia' LLM dissertation, University of Oslo, Norway, 2009
- EPIC Alert 'EPIC Hosts Privacy and Public Voice Conference in Africa' (23 December 2005) Vol 11, No 24, http://www.epic.org/alert/EPIC_Alert_11.24.html (accessed 10 November 2021)
- Evrensel, A 'Introduction' in Evrensel, A (ed) *Voter registration in Africa: A comparative analysis* (EISA 2010) 1

- Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series (2020), <https://ssrn.com/abstract=3582478> or <http://dx.doi.org/10.2139/ssrn.3582478>. (accessed 10 November 2021)
- Gross, H 'The concept of privacy' (1967) 42 *New York University Law Review* 34
- Gutwirth, S *Privacy and the information age* (Lanham/Boulder/New York/Oxford/Rowman & Littlefield Publ 2002)
- Izuogu, CE 'Data protection and other implications in the ongoing SIM card registration process' (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 10 November 2021)
- King, RU 'Healing psychological trauma in the midst of truth commissions: The case of Gacaca in post-genocide Rwanda' (2011) 6 *University of Toronto Press Journals* 134
- Knoll, M 'Budget support: A reformed approach or old wine in new skins?' UNCTAD Discussion Papers 190 (October 2008) 1
- Kusamotu, A 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46' (2007) 16 *Information and Communications Technology Law* 149
- Ladan, MT 'The Role of Law in the HIV/AIDS Policy:-Trend of Case Law in Nigeria and Other Jurisdictions', Inaugural Lecture delivered at the Ahmadu Bello University, Zaria, Nigeria, 2008, pp 1-64
- Makulilo, A.B., 'African accession to Council of Europe Privacy Convention 108: Moving towards stronger privacy protection' (2017) 41 *Datenschutz und Datensicherheit-DuD* 364
- Makulilo, AB 'Data protection and law reform in Africa: A systematic or flawed process?' (2016) 2 *International Journal of Technology Policy and Law* 228
- Makulilo, AB 'Data protection regimes in Africa: Too far from European "adequacy" standard?' (2013) 3 *International Data Privacy Law* 42
- Makulilo, AB 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer, Law & Security Review* 78
- Makulilo, AB 'Nigeria's Data Protection Bill: Too many surprises' (2012) *Privacy Laws & Business International Report* 25
- Makulilo, AB 'Registration of SIM cards in Tanzania: A critical evaluation of the Electronic and Postal Communications Act, 2010' (2011) 17 *Computer and Telecommunications Law Review* 48

- Makulilo, AB 'The quest for information privacy in Africa' (2018) 8 *Journal of Information Policy* 317
- Mbonu, NC and others 'Stigma of people with HIV/AIDS in sub-Saharan Africa: A literature review' *Journal of Tropical Medicine* 2009, Article ID 145891, 14 pagesdoi:10.1155/2009/145891
- McBride, WL 'The concept of justice in Max, Engels, and Others' (1975) 85 *Ethics* 204
- Neethling, J and others *Neethling's law of personality* (LexisNexis 2005)
- Neethling, J and others *Neethling's law of personality* (Butterworth 1996)
- Neethling, J 'Die reg op privaatheid' LLD thesis, UNISA, 1976
- Neethling, J 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18
- Rawls, J 'Justice as fairness' (1958) 62 *The Philosophical Review* 164
- Rawls, J *A theory of justice* (Harvard University Press 1971)
- Roos, A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 400
- Roos, A 'The law of data (privacy) protection: A comparative and theoretical study' LLD thesis, UNISA, 2003
- Sachs, D 'A fallacy in Plato's Republic' (1963) 72 *The Philosophical Review* 141
- Sutherland, E 'The mandatory registration of SIM cards' (2010) 16 *Computer and Telecommunications Law Review* 61
- Tadesse, MA 'HIV Testing from an African human rights system perspective: An analysis of the legal and policy framework of Botswana, Ethiopia and Uganda' LLM dissertation, University of Pretoria, 2007
- Warren, SD & Brandeis, LS 'The right to privacy' (1890) 4 *Harvard Law Review* 193
- Weiser, SD and others 'Routine HIV testing in Botswana: A population-based study on attitudes, practices, and human rights concerns' (2006) 3 *PLoS Medicine* 1013
- Weldon, G 'A comparative study of the construction of memory and identity in the curriculum of post-conflict societies: Rwanda and South Africa' (2003) 3 *International Journal of Historical Learning, Teaching and Research* 55
- Xu, H and others 'Examining the formation of individual's privacy concerns: Toward an integrative view' International Conference on Information Systems (ICIS) Proceedings (2008) 1

3

AN OLD QUESTION IN A NEW DOMAIN: SOME PRELIMINARY INSIGHTS ON BALANCING THE RIGHT TO PRIVACY AND FREEDOM OF EXPRESSION IN THE DIGITAL ERA UNDER THE AFRICAN HUMAN RIGHTS LAW

Yohannes Eneyew Ayalew

Abstract

This chapter seeks to examine how any exercise balancing the right to privacy with that of freedom of expression on the internet should be framed. The balancing of rights is a long-standing debate in human rights law discourse and is now being resurfaced on the internet domain. Courts in various jurisdictions have adopted several touchstones to balance the right to privacy and the right to freedom of expression. This chapter explores two contexts that are of significant current concern under the African human rights system: the publication of personal information and an individual's right to be forgotten. The first focus is the question of the publication of personal information about individuals where their private information is posted on the internet. Under this context, different factors, such as the contribution of the personal information to the general debate, the method of obtaining the information, how the person concerned is well-known, the prior conduct of the person, the content and form, and severity of the sanctions to be imposed, should be used to balance the right to privacy and expression. The right to be forgotten is the second context where the right to privacy is balanced against freedom of expression once the right holder requests the removal of content online where it is deemed prohibited under regional data protection laws. However, which right tipping the scale depends on a case-by-case basis. Ultimately, the chapter aims to offer some preliminary insights into the ways in which an appropriate balance should be struck between the right to privacy and freedom of expression within the African human rights system in the digital environment.

1 Introduction

The issue of balancing human rights may arise in situations where rights compete with one another or when rights conflict.¹ Rights can be understood in many ways and can be understood in absolute or relative terms. Whenever rights are understood as qualified entitlements (and not absolute rights) or along the lines of Raz's interest theory,² then conflicts

1 J Waldron 'Rights in conflict' (1989) 99 *Ethics* 503-519.

2 According to Raz, a person may be said to have a right if and only if some aspect

of rights must be regarded as inevitable. The utilitarian theory ('maximise happiness') customarily tends to resolve conflicts by giving precedence to happiness for the masses through sacrificing individual rights.³ To put it another way, utilitarian reasoning involves trade-offs between competing rights through prioritising public interests. On the other hand, Dworkin argues that the whole point of rights is to trump utilitarian claims that would permit the right to freedom of expression to be limited in the public interest⁴ since the right to freedom of expression should prevail over public interest unless in time of emergency.⁵

Whereas Mutua consistently views that the concept of duties under the African Charter is meant to strike a balance between rights and community/public interests.⁶ Mutua postulates the idea of the dialectic nature of rights and duties in Africa in that 'individual rights cannot make sense in a social and political vacuum, devoid of the duties assumed by individuals.'⁷

Etymologically, the term 'balance' comes from French yet has Latin origins, having evolved from a blend of 'bi' (meaning double) and 'lanx' (meaning having a two scale pans). Thus, the word 'balance' has the following dictionary meanings⁸:

a situation in which different things exist in equal, correct or good amounts; (2) an instrument for weighing things, with a bar that is supported in the middle and has dishes hanging from each end. [idiom] (3) to manage to find a way of being fair to two things that are opposed to each other; to find an acceptable position that is between two things.

Based on the above definitions, the word balance can be understood to send two significant messages. Firstly, an instrument of weighing things

of well-being (one's interest) is sufficiently important in itself to justify holding some other person(s) to be under a duty. See J Raz *The morality of freedom* (1986) 166.

3 Waldron (n 1) 507.

4 R Dworkin 'Rights as trumps' in J Waldron (ed) *Theories of rights* (1984) 153.

5 R Dworkin *Taking rights seriously* (1977) 195, 364.

6 See M Mutua, *Human rights: A political and cultural critique* (2002) 73-93; M Mutua, 'The Banjul Charter and the African cultural fingerprint: An evaluation of the language of duties' (1995a) 35 *Virginia Journal of International Law* 339, 340; and M Mutua 'Why redraw the map of Africa: A moral and legal inquiry' (1995b) 16 *Michigan Journal of International Law* 1146.

7 Mutua 1995a (n 6) 341.

8 Oxford Learners' Online Dictionary definition of the word 'balance' https://www.oxfordlearnersdictionaries.com/definition/english/balance_1?q=balance (accessed 24 August 2023).

that exist on equal footing. In one way, the courts examine one interest outweighing another.⁹ Under this view, the balancers (courts) place their interests on a set of scales and rule how the scales tip.¹⁰ For example, the right to privacy and freedom of expression can exist equally but be balanced and the decision maker may favour privacy instead of freedom of expression when the scale tips. Secondly, the decision-makers employ a different version of balancing when they speak of 'striking a balance' between or among competing rights.¹¹ Here, the decision-makers need to find a way of being fair to two things that are opposed to each other. Accordingly, one right does not override the other; rather, each right survives and is given its due. For instance, in striking a balance between privacy and freedom of expression, the decision maker would finally tilt to freedom of expression rather than privacy but set some modalities that the latter endures.

Habermas has argued that balancing 'deprives basic rights of their normative strength'¹² and, accordingly, the whole process of balancing relegates them to the status of values that must take their place among the range of policies facing legislators and administrators.¹³ There are no rational standards for balancing, so decisions on how to weigh, say, freedom of expression against national security become arbitrary or at least unpredictable.¹⁴ Refuting Habermas's claim, Alexy contends that courts can make rational judgments about the intensity of the interference with a right, for example, to freedom of expression under a public order law, and also about the respective importance in these contexts of competing rights.¹⁵

Balancing presupposes that human rights are not absolute but, rather, limited by a number of restrictions. This means that restrictions could be taken as a means to trade off other interests or rights. When rights are formulated in relative terms, we may face the inevitable balancing

9 TA Aleinikoff 'Constitutional Law in the Age of Balancing' (1987) 96 *Yale Law Journal* 946.

10 As above.

11 As above.

12 J Habermas *Between facts and norms* trans W Rehg (1996) 181, 256.

13 See M Rosenfeld & A Arato *Habermas on law and democracy: Critical exchanges* (1998) 381.

14 E Barendt 'Balancing freedom of expression and privacy: The jurisprudence of the Strasbourg Court' (2009) 1 *Journal of Media Law* 50.

15 R Alexy 'Constitutional rights, balancing, and rationality' (2003) 16 *Ratio Juris* 136. See also R Moosavian 'A just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7 *Journal of Media Law* 196-224, and D Julie 'Balancing Rights in a Democracy: The Problems with Limitations and Overrides of Rights under the Victorian Character of Human Rights and Responsibilities Act 2006' (2008) 32 *Melbourne University Law Review* 422, 424.

exercise.¹⁶ For example, freedom from torture is an absolute right, as there is no restriction that can hamper the enjoyment of the right. In such cases, the issue of balancing should not arise at all. When it comes to qualified rights, the balancing exercise is an inevitable task. For example, under the International Covenant on Civil and Political Rights (ICCPR), everyone has the right to privacy, but the right may be subject to reasonable and lawful interference.¹⁷ Similarly, the right to freedom of expression may be subject to various restrictions such as the rights or reputations of others (for instance, the right to privacy), the protection of national security, public order, and public health or morals.¹⁸ Hence, balancing rights is a significant weapon to trade-off competing rights.

However, critics claim that balancing rights can possibly squeeze the full enjoyment of rights or ‘swallow up the rights’ existence.¹⁹ To tackle the potential rights shrinkage, balancing exercises must show a strong commitment to the principle of proportionality.²⁰ This principle requires that the objective of public interest (utilitarian grounds) has to be sufficiently important to limit the right. Also, the measure of the limitation has to be suitable, must be appropriate to achieve their protective function, and must be the least intrusive instrument among those that might achieve their protective function.²¹

Balancing the right to privacy against the right to freedom of expression to determine which one precedes the other rests on the key normative assumption.²² Balancing rights over the internet, for example, in the case of the right to privacy and freedom of expression, is sufficiently addressed by the mechanics of the African human rights law and follows a similar *modus operandi* with offline balancing.²³ Nevertheless, this assumption is

16 B Cali ‘Balancing human rights: Methodological problems with weights, scales and proportions’ (2007) 29 *Human Rights Quarterly* 253.

17 UN General Assembly International Covenant on Civil and Political Rights, 16 December 1966, United Nations Treaty Series (UNTS) vol 999 171, art 17(1).

18 Art 19(3) ICCPR (n 17).

19 BB Lockwood, J Finn & G Jubinsky ‘Working Paper for the Committee of Experts on Limitation Provisions’ (1985) 7 *Human Rights Quarterly* 35-88.

20 UN Commission on Human Rights The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4, Principle 10. See Cali (n 16) 253.

21 UN Human Rights Committee (HRC) CCPR General Comment 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9 paras 14-15. See also M Fordham & T de la Mare ‘Identifying the principles of proportionality’ in J Jowell & J Cooper (eds) *Understanding human rights principles* (2000) 31.

22 Cali (n 16) 254.

23 This assumption receives additional resonance for the internet than Cali’s initial

not straightforward. Rather the relationship among the practical contexts, the underlying values of rights, and public interest aims is multifaceted and controversial.²⁴

In some contexts, the right to privacy and freedom of expression can be mutually reinforcing. The right to privacy reinforces the right to freedom of expression to the extent that privacy plays an important role in the creation of the content required to be expressed, thereby making possible the adequate exercise of freedom of expression.²⁵ Thus, Respect for privacy is a prerequisite for trust by those engaging in communicative activities, which is a pre-condition for exercising the right to freedom of expression.²⁶ Freedom of expression equally reinforces the right to privacy to the point that freedom of expression is critical to the protection of privacy.²⁷ For instance, freedom of information enables disclosures about large-scale data breaches and privacy invasions – an instance by behemoth tech companies – that may otherwise not be disclosed. As interdependent rights, freedom of expression and privacy also intersect over the question of protecting a person's reputation and defamation.²⁸

However, while the internet has opened new frontiers of freedom of expression, it is also eroding protections for privacy, necessitating a balance between the two rights. When one thinks of balancing the right to privacy and freedom of expression, the balancing exercise remains an arduous task as it requires many factors to weigh these rights. Courts in various jurisdictions have used touchstones to balance these competing rights.²⁹ The process of balancing both rights is not linear. Thus far, except for the South African case law, there is no rich jurisprudence regarding balancing the right to privacy against freedom of expression under African human rights law. Instead, the chapter draws upon European human rights law or elsewhere for illustrative purposes. Hence, using a lesson-drawing perspective mainly from that of European human rights law, the chapter explores two contexts: the publication of personal information

propositions.

24 Cali (n 16) 255.

25 OHCHR Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue (17 April 2013) UN Doc. A/HRC/23/40.

26 T Mendel and others *Global survey on internet privacy and freedom of expression* UNESCO Series on Internet Freedom, Paris: UNESCO (2012) 95.

27 J Cannataci and others 'Privacy, free expression and transparency and redefining their new boundaries in the internet ecosystem' UNESCO Internet Study (2016) 79.

28 E Barendt 'Privacy and freedom of speech' in AT Kenyon & M Richardson (eds) *New dimensions in privacy law: International and comparative perspectives* (2006) 11-31.

29 Barendt (n 14) 14.

and an individual's right to be forgotten. The first focus is the question of the publication of personal information about individuals where their private information is posted on the internet. The chapter discusses several factors.³⁰ Some of these factors include: the contribution of the personal information to the general debate, the method of obtaining the information, how the person concerned is well-known, prior conduct of the person, the content, consequence and form of the publication, and severity of the sanctions to be imposed are used to balance the right to privacy and expression. However, which right tips the scale depends on a case-by-case basis.

The chapter is structured in six sections, including this introduction. The second section will discuss the normative protection of internet freedom in Africa. Following this, a discussion will be made on the legal protection of the right to privacy and the right to freedom of expression in the African human rights ecosystem. The third section briefly explores the idea of balancing the right to privacy and freedom of expression on the Internet. How the publication of individuals' personal information has become a *causes célèbre* in striking an appropriate balance between the right to privacy and freedom of expression, and will be discussed extensively under section four. Section five examines the nuances of the right to be forgotten, and its niche in balancing competing rights on the internet. The chapter concludes by offering few preliminary thoughts on how to strike an appropriate balance between the right to privacy and freedom of expression under the African human rights law.

2 Internet freedom under the African human rights law

The advent of the internet in Africa is a recent phenomenon. The first network in sub-Saharan Africa arrived in 1988 at Rhodes University in Grahamstown, South Africa.³¹ Following it, in 1991, the first data packet transmitted from sub-Saharan Africa was sent from South Africa to Portland, Oregon, which, in turn, heralded the arrival of the internet to Africa.³²

30 See *Axel Springer AG v Germany* European Court of Human Rights (ECtHR) Strasbourg, Application 39954/08, 7 February 2012 paras 89-95; see also *Von Hannover v Germany* (No 2) ECtHR, 12 February 2012 App 40660/08 and 60641/08, paras 108-113.

31 T Nyirenda-Jere & T Biru 'Internet development and internet governance in Africa' (Internet Society, May 2015) 6.

32 As above.

In the past two decades African countries have experienced a steady growth in internet penetration, from 0.78 per cent in 2000 to 43.3 per cent in 2023, with an estimated 590 million people using the internet.³³ Yet, as of 31 December 2022, the number of internet users in Europe was estimated at around 87.7 per cent of the population. This translates to about 727.5 million people, almost twice as many in Africa.³⁴ Thus, Africa still lags behind the rest of the world in internet penetration since it is still well below the global average of 64.2%.³⁵ As such, African states should work more towards rapidly bridging the gap.

The use of the internet is speedily increasing across the African continent, with millions of individuals getting online and engaging in a wide range of usages of social media and other digital platforms for varying purposes – including in relation to political matters and for governance, social and economic development.³⁶ This development has the potential to further the right to freedom of expression but can come at the cost of other rights, including privacy. The central question underlying this chapter is how to achieve an appropriate balance between the right to privacy and freedom of expression on the internet under the African human rights law.

With the expanding pace of internet penetration in Africa, internet freedom has been subjected to different measures by state or non-state actors, resulting in muzzling freedom of expression on the internet and breaching data privacy. For example, it has been claimed that most governments in Africa have turned to internet shutdowns as a tool of political hegemony and for political control.³⁷ To put it another way, most governments are more than ever using digital technologies with private contractors to surveil, censor and suppress fundamental and basic

33 International Telecommunications Union Global and Regional ICT Data <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (accessed 20 July 2023). See also Internet World Stats, Internet Penetration in Africa (31 December 2022) <https://www.internetworldstats.com/stats1.htm> (accessed 13 November 2023).

34 As above.

35 As above

36 African Declaration on Internet Rights and Freedoms, launched at the 18th annual Highway Africa Conference at Rhodes University, Grahamstown, South Africa, 7 September 2014, <http://africaninternetrights.org/articles/> (accessed 24 August 2023).

37 F Erixon & H Lee-Makiyama 'Digital authoritarianism: Human rights, geopolitics and commerce' European Centre for International Political Economy (ECIPE), ECIPE Occasional Paper 5/2011 (2011) 1, <http://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf> (accessed 24 August 2023).

freedoms of their people through censorship, filtering, blocking, targeted and targeted and mass surveillance and internet shutdowns.³⁸

Internet freedom is a catchphrase referring to human rights in the digital age, particularly access to the internet. Yet, the claim of internet freedom (including access to the internet) as a separate human right remains unsettled.³⁹ There are contending debates about whether access to internet is a human right. For example, La Rue supports the notion of internet access as a human right since the internet has become a vital communication medium that individuals can use to exercise their right to freedom of expression.⁴⁰ On the contrary, Cerf argues that internet access is not a human right. He contends that 'technology is an enabler of rights, not a right itself.'⁴¹ Other authorities claim that access to the internet is not a human right *stricto sensu* but rather a derivative human right since it enhances the exercise of freedom of expression per the ruling by the *Economic Community of West African States (ECOWAS) Community Court of Justice in Amnesty International Togo and Others v Republic of Togo*.⁴²

Traditionally, internet freedom is framed narrowly as the right of access to the internet. According to the former United Nations (UN) Special Rapporteur on the right to freedom of expression, La Rue, access to the internet has at least two dimensions, namely, access to content (without the arbitrary and unwarranted filtering or blocking of content)⁴³ and access to the infrastructure and equipment required to use the internet.⁴⁴ However, internet freedom is a metaphoric term used to convey various rights in the digital age, such as the right to freedom of expression⁴⁵ and the right to

38 See A Mare 'Internet shutdowns in Africa: State-ordered internet shutdowns and digital authoritarianism in Zimbabwe' (2020) 14 *International Journal of Communication* 4244..

39 S Tully 'A human right to access the internet? Problems and prospects' (2014) 14 *Human Rights Law Review* 180. See AA Gillespie 'Restricting access to the internet by sex offenders (2011) 19 *International Journal of Law and Information Technology* 171, 184.

40 UN Special Rapporteur (n 25) para 10. See also the UN Human Rights Council's affirmation that rights must be protected online. Human Rights Council 'The promotion, protection and enjoyment of human rights on the internet' A/HRC/20/L.13, 5 July 2012.

41 VG Cerf 'Internet access is not a human right' *New York Times* (4 January 2012), <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html> (accessed 30 August 2023).

42 *Amnesty International Togo & Others v Republic of Togo* ECOWAS Community Court of Justice, JUD ECW/CCJ/JUD/09/20 (25 June 2020) para 38.

43 See the Report of the UN Special Rapporteur (n 25) paras 2 & 10.

44 UN Special Rapporteur (n 25) para 61.

45 See M Land 'Toward an international law of the internet' (2013) 54 *Harvard International Law Journal* 393, 457.

communicate,⁴⁶ privacy,⁴⁷ the right to peaceful assembly⁴⁸ and access to the internet.⁴⁹ In this respect, Joyce submits that internet freedom plainly ‘involves more than questions of infrastructure and the architecture of the internet, and engages with key human rights principles such as freedom of expression, privacy and even security’.⁵⁰

The right to privacy is an important entitlement on the internet domain that requires legal protection, as it is under constant encroachment from governments, for example, rapidly introducing digitalisation, e-government and digital identity programmes and from private actors who aggregate, collect and process personal data without lawful means. It is arising more acutely in the internet as it requires citizens to provide detailed personal information online, for example, biometrics for voters’ cards, SIM card registration, identity cards, and driver’s licences, among others.⁵¹ In 2015, the UN Human Rights Council adopted a landmark resolution that recognises the right to privacy in the digital age by affirming that: ‘the same rights that people have offline must also be protected online, including the right to privacy.’⁵² Crucially, while interpreting the right to privacy under Article 16 of the Convention on the Rights of the Child, the UN Committee on the Rights of the Child has clarified that the right to privacy may be exercised in the digital environment.⁵³

46 D Joyce ‘Internet freedom and human rights’ (2015) 26 *European Journal of International Law* 493-514.

47 Report of the Office of the United Nations High Commissioner for Human Rights The right to privacy in the digital age A/HRC/27/37 (30 June 2014) paras 12-14. See also UN Human Rights Council Resolution 28/16, The right to privacy in the digital age A/HRC/RES/28/16 (1 April 2015) art 3: ‘The same rights that people have offline must also be protected online, including the right to privacy.’

48 See UN Human Rights Committee, General Comment 37 art 21: right of peaceful assembly, CCPR/C/GC/37 (27 July 2020) para 34.

49 UN Special Rapporteur (n 25) para 2.

50 Joyce (n 46) 506.

51 The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Mapping Trends in Government Internet Controls, 1999-2019 (September 2019) 5.

52 UN Human Rights Council Resolution 28/16, The right to privacy in the digital age, A/HRC/RES/28/16 (1 April 2015) para 3. See also Report of the Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/27/37 (30 June 2014) Paras 12-14. On the United Nations General Assembly’s Resolution 68/167 on the right to privacy in the digital age, see generally D Joyce, ‘Privacy in the Digital Era: Human Rights Online?’ (2015) 16 *Melbourne Journal of International Law* 1-15.

53 UN Committee on the Rights of the Child (UNCRC), General comment No. 25 (2021) on children’s rights in relation to the digital environment, CRC/C/GC/25 (2 March 2021) para 67-79.

Freedom of expression is a linchpin right that enables individuals to participate in a democracy⁵⁴ and is also a key to the realisation of other human rights.⁵⁵ This role has traditionally been performed by the print media and broadcasters, but online media through the internet is transforming our lives and giving a voice to millions of people in Africa.⁵⁶ The internet provides a mechanism for amplifying its exercise in many African countries.⁵⁷ For example, the internet in some cases has enabled Africans to replace despotic and dictatorial rulers. For instance, the internet played a role in popular revolutions in Egypt,⁵⁸ Ethiopia,⁵⁹ Sudan⁶⁰ and Tunisia.⁶¹ In relation to freedom of expression on the internet, the emerging concerns include a lack of internet access; draconian national security laws; blanket content filtering; wholesale blackouts; hate speech; and disinformation regulation.⁶²

The African human rights law provides a normative framework for the protection of the rights to privacy and freedom of expression on the internet in its different instruments. However, the African Charter on Human and Peoples' Rights (African Charter) does not contain an explicit provision

- 54 UN Human Rights Committee (HRC) General comment 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34, para 2 <http://www.refworld.org/docid/4ed34b562.html> (accessed 21 February 2019).
- 55 E Barendt *Freedom of speech* (2007) 18-21; J Cannataci and others 'Privacy, free expression and transparency and redefining their new boundaries in the internet ecosystem' UNESCO Internet Study, 2016.
- 56 Media Legal Defence Initiative (MLDI) 'Mapping digital rights and online freedom of expression in East, West and Southern Africa' (2018) 10-14, https://10years.mediadefence.org/wp-content/uploads/2019/07/Mapping-digital-rights-litigation_Media-Defence_Final.pdf (accessed 24 August 2021). See also D McGoldrick 'The limits of freedom of expression on Facebook and social networking sites: A UK perspective' (2013) 13 *Human Rights Law Review* 125, 151.
- 57 A Puddephatt *Freedom of expression and the internet* (UNESCO 2016) 17.
- 58 See Frank la Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, A/HRC/17/27 (16 May 2011) para 4; K Clarke & K Kocak 'Launching revolution: Social media and the Egyptian uprising's first movers' (2020) 50(3) *British Journal of Political Science* 1025.
- 59 A Bitew 'Social media and the simmering Ethiopian revolution' ECDAF (3 September 2016), <https://ecadforum.com/2016/09/03/social-media-and-the-simmering-ethiopian-revolution-alem-bitew/> (accessed 24 August 2021).
- 60 N Taha 'Sudan's social media deemed major player in Bashir's ouster' *VOA News* 18 April <https://www.voanews.com/a/sudan-s-social-media-deemed-major-player-in-bashir-s-ouster-/4882059.html> (accessed 24 August 2021).
- 61 A Dhillon 'Social media and revolution: The importance of the internet in Tunisia's uprising' (2014) *Independent Study Project (ISP) Collection* 1-21.
- 62 See Y Ayalew 'Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights' (2020) 20 *African Human Rights Law Journal* 315.

on the right to privacy but addresses the right to privacy impliedly as part of the right to integrity and life under article 4, right to dignity under article 5, the right to security and liberty under article 7 and the right to health under article 16 of the African Charter. Also, there is a growing understanding that the right to privacy⁶³ can be read under the African Charter through the right to dignity⁶⁴ and the right to liberty and security of a person.⁶⁵ The concept of dignity is consubstantial, intrinsic and inherent to the human person.⁶⁶ This means that dignity empowers individuals to feel honour or respect to the extent of protecting their privacy.⁶⁷ However, other relevant instruments that provide for the right to privacy include the African Charter on the Rights and Welfare of the Child (African Children's Charter),⁶⁸ the African Union Convention on Cyber Security and Personal Data Protection;⁶⁹ the Personal Data Protection Guidelines for Africa;⁷⁰ and the African Declaration on Freedom of Expression and Access to Information.⁷¹

Regional economic communities (RECs) have adopted measures to protect the right to privacy. For example, the East African Community (EAC) adopted a Framework for Cyber Laws to guide its member states on regional and national processes to facilitate a harmonised legal regime on privacy and data protection.⁷² In addition, in 2010, ECOWAS adopted

63 See A Singh & M Power 'The privacy awakening: the urgent need to harmonise the right to privacy in Africa' (2019) 3 *African Human Rights Yearbook* 211; see also YE Ayalew, 'Untrodden paths towards the right to privacy in the digital era under African human rights law,'(2022) 12 *International Data Privacy Law* 16-32.

64 Art 5 Organisation of African Unity (OAU) African Charter on Human and Peoples' Rights (African Charter) 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (African Charter).

65 Arts 4 and 6 African Charter.

66 *Open Society Justice Initiative v Côte d'Ivoire*, (ACHPR), Communication 318/06, 27 May 2016, para 139.

67 See R Murray, *The African Charter on Human and Peoples' Rights a Commentary* (Oxford University Press, 2019) 138.

68 Organisation of African Unity (OAU) African Charter on the Rights and Welfare of the Child 11 July 1990, CAB/LEG/24.9/49 (1990), art 10.

69 Art 8 African Union Convention on Cyber Security and Personal Data Protection ('Malabo Convention'), opened for signature in 27 June 2014, entered into force 8 June 2023.

70 See the Personal Data Protection Guidelines for Africa (2018), Internet Society and the African Union.

71 Principle 40 Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) Lawrence Mute, Special Rapporteur on Freedom of Expression and Access to Information in Africa.

72 Art 19 Draft East African Community (EAC) Legal Framework for Cyber Laws (2008).

the Supplementary Act on Personal Data Protection, which urges member states to establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the state.⁷³ Similarly, in an effort to harmonise data protection laws in Southern Africa, the Southern African Development Community (SADC) published the SADC Model Law on Data Protection in 2013.⁷⁴

The African Charter recognises the right to freedom of expression⁷⁵ but subject to legitimate limitations.⁷⁶ The jurisprudence of the African Commission on Human and Peoples' Rights (African Commission) regarding the right to freedom of expression on the internet is still developing. However, the Commission has already decided on some important communications – on a free press,⁷⁷ expressed through any form of media,⁷⁸ and the right to publish an article on the internet.⁷⁹ Additionally, a few developments have been observed in Africa aimed at enhancing the right to privacy and freedom of expression on the internet, at least in the form of soft law. For instance, inspired by the landmark UN Human Rights Council Resolution,⁸⁰ the African Commission Resolution on Freedom of Information and Expression on the Internet has urged African states to respect the right to freedom of expression on the internet through implementing legislative and other measures.⁸¹

73 Art 2 Supplementary Act on Personal Data Protection within Economic Community of West African States (ECOWAS) 2010.

74 Southern African Development Community (SADC) Model Law: Data Protection (2013).

75 Art 9 African Charter.

76 Arts 9(2) & 27 African Charter.

77 *Article 19 v Eritrea* (2007) AHRLR 73 (ACHPR 2007) para 107.

78 *MonimElgak, Osman Hummeida and Amir Suliman (represented by FIDH and OMCT) v Sudan* Communication 379/09, ACHPR) para 114.

79 *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development in Africa (on behalf of Andrew Barclay Meldrum) v Zimbabwe* (ACHPR 294/04) paras 3, 110-112.

80 The promotion, protection and enjoyment of human rights on the Internet: resolution adopted by the Human Rights Council, 18 July 2016, A/HRC/RES/32/13 para 1.

81 Art 1 African Commission on Human and Peoples' Rights (the Commission), Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016, meeting at its 59th Ordinary Session, held Banjul, Islamic Republic of the Gambia, from 21 October to 04 November 2016. See preamble para IX "Further recognizing that privacy online is important for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."

Internet access is a mechanism to ensure internet freedom. To this end, the African Declaration emphasised that a universal, equitable, affordable and meaningful access to the internet is necessary for realising freedom of expression.⁸² In this respect, African states have a positive obligation to adopt laws, policies and other measures to provide universal, equitable, affordable and meaningful access to the internet without discrimination.⁸³ First, states should develop independent and transparent regulatory mechanisms for effective oversight. Second, states should improve information and communication technology and internet infrastructure for universal coverage.

In Africa the digital divide – where individuals and communities experience uneven distribution of access to the internet – is still unequal. States should endeavour to bridge these gaps. African states set Agenda 2063 as a noble initiative to tackle the socio-economic challenges and transform the continent into development, pursued under Ppan-Africanism and African Renaissance.⁸⁴ For instance, it aspires to a digital economy, and connecting Africa through high-speed internet.⁸⁵ Similarly, universal internet access is one of the aspirations that states commit to achieving under the UN Sustainable Development Goals (SDGs).⁸⁶

Lastly, the most significant contribution of the African Declaration is how it recognises the need to balance the right to privacy and freedom of expression. In the Preamble, the Declaration underscores that the right to privacy and freedom of expression are mutually-reinforcing rights.⁸⁷ Likewise, the right to privacy and freedom of expression may conflict, and in such cases a proper balance should be struck. This chapter has identified two contexts, namely, publication of personal information⁸⁸ and the right to be forgotten,⁸⁹ found in the African Declaration, which merit a

82 Principle 37(2) African Declaration.

83 Principle 37(3) (n 65 above) African Declaration.

84 African Union, Agenda 2063: The Africa We Want (African Union Commission 2015).

85 As above, paras 25 and 72 (g): 'ICT: A continent on equal footing with the rest of the world as an information society, an integrated e-economy where every government, business and citizen has access to reliable and affordable ICT services by increasing broadband penetration by 10% by 2018, broadband connectivity by 20 percentage points and providing access to ICT to children in schools and venture capital to young ICT entrepreneurs and innovators and migration to digital TV broadcasting by 2016.'

86 UN General Assembly Transforming our world: The 2030 Agenda for Sustainable Development 21 October 2015, A/RES/70/1, goal 9 target 9(c).

87 Preamble para XVIII African Declaration.

88 Principle 26 African Declaration.

89 Principle 42(3)(d) African Declaration.

further discussion for balancing freedom of expression and privacy rights in sections 4 and 5.

3 Balancing the right to privacy and freedom of expression: Preliminary insights

The advent of balancing competing rights dates back to the late 1950s to early 1960s through a series of synchronous decisions by the German Constitutional Court⁹⁰ and the US Supreme Court.⁹¹ In these early judgments, balancing was first referred to and discussed in the area of the right to freedom of expression adjudication. The US and German courts have influenced the contemporary understanding of balancing rights as seen in other states such as the United Kingdom.⁹²

The balancing of rights implies an image of weights assigned to values in rights and a head-to-head comparison of these weights.⁹³ Technically, acts of balancing require ‘identification, valuation, and comparison of competing of interests’, assigning values to them and ultimately to deciding which interest yields the net benefit.⁹⁴

Balancing rights involves understanding the values that societies highly prioritise. Koskeniemi argues that any sort of balancing rights will involve broad cultural and political assumptions about whether the society should prefer the values of public order, individual rights or the right that better outweighs.⁹⁵ This means that states give cultural and political assumptions in upholding one right than the other. For example, in the US legal system, the right to free speech is given precedence than any right as the country’s long tradition of civil liberties and self-expression.

90 See *Lüth* case, Federal Constitutional Court (First Senate) 15 January 1958 BVerfGE 7 198.

91 See *Barenblatt v United States* 360 US 109 (1959); *Konigsberg v State Bar of California* 366 US 36 (1961); *Communist Party v Subversive Activities Control Board* 367 US 1 (1961). For a detailed analysis, see J Bomhoff *Balancing constitutional rights: The origins and meanings of post-war legal discourse* (2013) 28, 72.

92 See a number of cases that evolved in the UK addressing balancing rights: *Campbell v MGN* [2004] UK House of Lords 22 [107]; the decisions of the Court of Appeal in *Douglas v Hello! (No 6)* [2006] QB 125, in *McKennitt v Ash* [2008] QB 73, and in *Murray v Express Newspapers plc* [2008] EMLR 12, *Mosley v News Group Newspapers Ltd* [2008] EMLR 20, *Spelman v Express Newspapers* [2012] EWHC 355 [48], and *Sir Cliff Richard v The British Broadcasting Corporation and The Chief Constable of South Yorkshire Police*, Royal Court of Justice, Case HC-2016-002849, UK, 18 July 2018.

93 TA Aleinikoff ‘Constitutional law in the age of balancing’ (1987) 96 *Yale Law Journal* 945.

94 See Cali (n 10) 259 and Aleinikoff (n 93) 945.

95 M Koskeniemi *The politics of international law* (Bloomsbury Publishing, 2011) 144.

However, in the European setting, both the right to privacy and freedom of expression enjoy legal protection.

On the other hand, the African Charter provides the right to freedom of expression but not privacy. The early draft of the African Charter on Human and Peoples' Rights, which Kéba Mbaye drafted in 1979, contains an explicit provision on the right to privacy.⁹⁶ However, the final adopted draft of the African Charter on Human and Peoples' Rights contained no clear provision dedicated to the right to privacy when it was adopted in Banjul in 1981. It is unclear why the right to privacy was dropped in the final adopted version of the African Charter. Perhaps the reasons might be linked to two factors. One possible explanation is found in the Dakar Draft where drafters were fully convinced that peoples' rights should be inserted beside individual rights. They stated: 'The conception of an individual who is utterly free and utterly irresponsible and opposed to society is not consonant with African philosophy.'⁹⁷ The other reason could be when various delegates raised the concern during the second ministerial conference of the OAU that the Charter must reflect African traditional values.⁹⁸ This view was later accepted, and to this effect, a preambular provision was inserted in the final text.⁹⁹ Arguably, given an absence of an explicit provision on the right to privacy under the African Charter, the framers of the African Charter perhaps had assigned more value to free speech than privacy.

Based on the case laws of the European Court of Human Rights, one can draw the following balancing techniques. First, the traditional balancing exercise starts with a presumption in favour of either the right to privacy or of the right to freedom of expression – depending on the provision of the European Convention is invoked by the applicant.¹⁰⁰

96 Art 24 The Kéba Mbaye Draft on African Charter on Human and Peoples' Rights prepared for the Meeting of Experts in Dakar, Senegal from 28 November to 8 December 1979, CAB/LEG/67/1.

97 See [Dakar Draft] African Charter on Human and Peoples' Rights, Preliminary draft of the African Charter prepared during the Dakar Meeting of Experts at the end of 1979. CAB/LEG/67/3/Rev. 1., third governing principle.

98 Second Session of OAU Ministerial Conference on the Draft African Charter on Human and Peoples' Rights (Banjul The Gambia 7 - 19 January 1981) introduction, para 1.

99 African Charter para V 'Taking into consideration the virtues of their historical traditions and the values of African civilisation which should inspire and characterise their reflections on the concept of human and peoples' rights'.

100 Eg, in the first *Von Hannover* case itself, that a national judgment in favour of the press in a privacy case failed to respect her rights under art 8. See *Von Hannover v Germany* (1st case) ECtHR Application 59320/00 judgment, Strasbourg, 24 June 2004, paras 79-80. See dissenting opinion of Schäffer J in the case of *Pfeifer v Austria* ECtHR

Then, it requires ‘the state to show that the interference with the exercise of that right is necessary in a democratic society to protect the rights and freedoms of others’.¹⁰¹ Second, the issue of balancing could be resolved through the concept of ‘margin of appreciation’ doctrine, where the European Court tends to defer matters to the will of states since national authorities better know the local contexts.¹⁰² Third, the issue of balancing may be resolved through employing a matrix of several touchstones such as contribution of the personal information to the general debate, the method of obtaining the information, the how the person concerned is well-known, method of obtaining the information and its veracity, the content, form and consequences of the publication and the severity of sanctions imposed, which are discussed at length under section 4.

In Africa, states such as South African have some established jurisprudence in balancing competing rights.¹⁰³ In the case of *South African Broadcasting Co v Thatcher*¹⁰⁴ the South African High Court has granted a broadcasting company access to record legal proceedings and determined that courts should adopt a flexible approach that favours justice, and fairness, and based on the principle of proportionality subject to limitations applicable¹⁰⁵ when balancing the right to privacy with the right to freedom of expression.¹⁰⁶ In the same way, in the matter of *Tshabalala-Msimang & Another v Makhanya & Others*¹⁰⁷ the South African

(Application 12556/03) 15 November 2007, Judgment, Strasburg, para 5. ‘Where both values are at stake, the result of the Court’s balancing exercise ought not to depend on which particular article of the Convention has been relied on in the case before it.’

101 Barendt (n 14) 58.

102 The margin of appreciation should in principle be the same in both the right to privacy and freedom of expression. This means that contracting states enjoy a certain margin of appreciation in assessing whether and to what extent an interference with these rights guaranteed under each provision is necessary. See *Fürst-Pfeifer v Austria* (Applications 33677/10 and 52340/10) Judgment 17 May 2016 para 40; *Axel Springer AG v Germany* ([GC] 39954/08, para 87, 7 February 2012) and *Delfi AS v Estonia* [GC] 64569/09, para 139, 16 June 2015.

103 See PM Bekker & AG Janse van Rensburg ‘Balancing freedom of expression and the right to the privacy of medical data and information – The winner does not take all: *Mantombazana Edmie Tshabalala-Msimang & Medi Clinic v Makhanya*’ (2010) 73 *Journal for Contemporary Roman-Dutch Law* 41-60.

104 *South African Broadcasting Co v Thatcher* High Court of South Africa for the Cape of Good Hope Provincial Division, Case 8924/2004, 31 August 2005 paras 1-2: ‘The South African Broadcasting Company (SABC) requested the right to televise the proceedings against Mark Thatcher, who was on trial for his involvement in an attempted coup in Equatorial Guinea.’

105 *Thatcher* case (n 104) paras 110-111.

106 *Thatcher* case (n 104) para 118.

107 *Tshabalala-Msimang & Another v Makhanya & Others* (18656/07) 2008 (3) BCLR 338 (W) paras 6-9. ‘An article was published in the *Sunday Times* with the heading ‘Manto

High Court has found that respondents' right to freedom of expression – on the basis that the disclosure of information is in the public interest – weighed more than the first applicant's right to privacy.¹⁰⁸ The first applicant's right to privacy in her capacity as a public figure is not an absolute constitutionally protected right and can be limited under section 36 of the Constitution. Therefore, the Court resolved the balancing of competing rights through applying common limitation clauses under the Constitution. In the next section, I turn to the first context of balancing the rights to freedom of expression and to privacy in the digital environment, i.e., the publication of personal information.

4 Publication of personal information

The issue of balancing has traditionally been common in the context of the publication of personal information about individuals. When an individual's personal information relating to personal identity,¹⁰⁹ for example, photographs, medical information, contact details, or financial records, is published by online media, hounding press outlets or tabloid magazines, the right to privacy (reputation) of individuals may easily be tampered. The question is how an appropriate balance can be struck between the right of the press to freedom of expression and individuals' privacy.

The African Declaration provides the modalities of individuals' access to information whereby individuals have the right to access information held by public and relevant private bodies including proactive disclosure,¹¹⁰ in a prompt and inexpensive manner.¹¹¹ The access may also include personal information in published works although its application would give rise to a conflict with the right to privacy.

The publication of personal information has acquired additional resonance in the context of the internet because it enables the sharing and disseminating personal information to large sections of society at a time.

's hospital booze binge'. It was alleged that according to the first applicant's medical records she consumed alcohol on various occasions while she was treated with prescription drugs namely painkillers and sleeping tablets while hospitalised in one of the branches of the Medi-Clinic Group. The first applicant was at the time of the alleged infringement of her right to privacy of medical records and data, the Minister of Health and a member of the cabinet of the Government of the Republic of South Africa.'

108 *Tshabalala-Msimang* (n 107) para 44.

109 *Von Hannover v Germany* (n 30) para 50.

110 African Declaration Principle 29.

111 African Declaration Principle 26(1).

One of the overarching problems of the digital age is the unnecessary sensationalism of news or information virtually at times when individuals or the media access information. Although this touchstone varies in individual cases, unnecessary sensationalism of information while expressing one's right to freedom of expression arguably infringes the right to privacy.¹¹²

In *Axel Springer v Germany* the European Court indicated that several touchstones should be used to balance the right to freedom of expression and privacy in the context of media stories about persons.¹¹³ Using similar standards, in 2017 the European Court in the case of *Einarsson v Iceland*¹¹⁴ held that a balance should be tilted in favour of the right to privacy over the right to freedom of expression on the internet domain in the context of an Instagram post accusing the applicant of committing a rape.¹¹⁵ These include the contribution to the debate of general interest, how well-known is the person concerned and what is the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, content, form and consequence of the publication, and severity of the sanction imposed.

Accordingly, the first factor to be considered in weighing the right to privacy against freedom of expression in the context of publication of personal information is the contribution to a debate of general interest. This means publishing the alleged photos or articles must contribute to a debate of general interest.¹¹⁶ However, the question of what constitutes a subject of general interest will depend on the circumstances of the case. For example, the European Court considers the existence of general interest where the publication concerned focuses on political matters or criminal

112 *Sir Cliff Richard v The British Broadcasting Corporation and The Chief Constable of South Yorkshire Police*, Royal Court of Justice, Case HC-2016-002849, United Kingdom, 18 July 2018, paras 276, 318, 446(c). "the court found that the manner of reporting chosen by the BBC was to give great emphasis to the news as they decided to add sensationalism by using the helicopter."

113 *Axel Springer AG v Germany* (n 30) paras 89-95; see also *Von Hannover v Germany (No 2)* (n 30), para 108-113.

114 *Einarsson v Iceland* (Application 24703/15) [2017] ECHR 7 November 2017 para 53.

115 *Einarsson* (n 114) para 8.

116 *Axel Springer AG v Germany* (n 30) para 90; *Minelli v Switzerland* (dec.), ECHR no. ECtHR 14991/02, 14 June 2005.

issues,¹¹⁷ an article in the online archive of the newspaper,¹¹⁸ and sporting issues or performing arts.¹¹⁹ Yet, the marital or financial difficulties of the head of states or famous singers were not deemed to be matters of general interest.¹²⁰

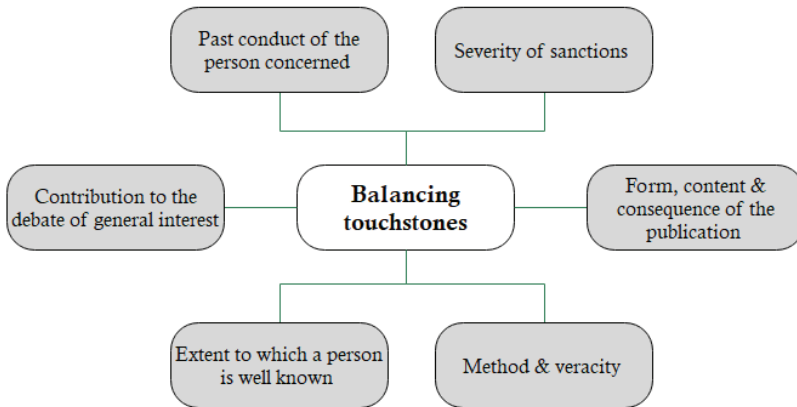


Figure 1: Publication of personal information and balancing touchstones adopted by the European Court of Human Rights (source: author)

The second factor is the extent to which the person concerned and the subject of the report are well-known. In the case of celebrities,¹²¹ political or public figures which are generally known to the public, unlike private individuals who are unknown to the public, may not often claim protection of privacy.¹²² However, the public's right to be informed may be limited – 'where the published photos relate exclusively to details of the public figures' private life and have the sole aim of satisfying the curiosity of a

117 *White v Sweden* 42435/02, ECtHR para 29, 19 September 2006; *Egeland and Hanseid v Norway* ECtHR 34438/04, 16 April 2009, para 58; *Leempoel & S.A. ED Ciné Revue v Belgium* ECtHR 64772/01, 9 November 2006 para 72; and *Einarsson v Iceland* (n 114 above) para 45.

118 *Fuchsman v Germany* ECtHR Application no. 71233/13 paras 38-39, 2017.

119 *Nikowitz and Verlagsgruppe News GmbH v Austria* ECtHR 5266/03 para 25, 22 February 2007; *Colaço Mestre and SIC – Sociedade Independente de Comunicação, SA v Portugal* ECtHR 11182/03 and 11319/03, para 28, 26 April 2007; and *Sapan v Turkey*, ECtHR 44102/04, para 34, 8 June 2010.

120 *Standard Verlags GmbH v Austria (No 2)* 21277/05 para 52, 4 June 2009, and *Hachette Filipacchi Associés (ICI PARIS) v France* 12268/03 para 43, 23 July 2009.

121 See generally P Loughlan and others *Celebrity and the Law* (The Federation Press, 2010) 125.

122 *Axel Springer AG v Germany* (n 30) para 91.

particular readership in that respect'.¹²³ In terms of the subject of report, the European Court pointed out a guidance on *Einarsson v Iceland (Instagram case)* that the matter was an altered picture of the applicant published on X's Instagram account along with the caption 'F**k you rapist bastard', after two rape charges against the applicant had been dropped.¹²⁴ As stated in the facts, X published an altered picture of the applicant on Instagram by drawing an upside-down cross on the applicant's forehead and writing "loser" across his face with the above caption while apparently, he had believed that only his friends who were his "followers" on Instagram, had access to the pictures that he published. But his pictures were also accessible to other Instagram users.¹²⁵

The third factor to be considered in balancing privacy and freedom of expression is the prior conduct of the person concerned. Simply put, when individual's photos or any personal information have already appeared in an earlier publication, these prior conducts need to be considered.¹²⁶ For example, in the Instagram case the European Court ruled that the applicant had prior conduct in terms of professional activities such as online writing, publication of books, appearances on television and experience in presenting oneself in the media.¹²⁷ Nevertheless, the mere fact of having experience with the press in previous events cannot bar the person concerned from protection against the publication of personal information.¹²⁸

The method of obtaining the information and its veracity is another significant factor to consider in balancing rights. This means that press or journalists have to exercise good faith in finding information and provide accurate and, reliable information as per the ethics of journalism.¹²⁹ However, the South African High Court in *Tshabalala-Msimang and Another v Makhanya* and Others found that the publication of unlawfully-obtained controversial information relating to a politician in the exercise of State functions is capable of contributing to a debate in a democratic society.¹³⁰

123 *Von Hannover v Germany* (no. 2) (n 29 above) para 65; *Standard Verlags GmbH v Austria (No 2)* 21277/05, para 53, 4 June 2009).

124 *Einarsson* (n 114) para 43.

125 *Einarsson* (n 114) para 8 and 9.

126 *Hachette Filipacchi Associés* (n 113) paras 52-53.

127 *Einarsson* (n 114) para 43.

128 *Egeland and Hanseid* (n 110) para 62, *Von Hannover (No 2)* (n 28) para 111.

129 *Fressoz and Roire v France* [GC] 29183/95 para 54, ECHR 1999-I; *Stoll v Switzerland* [GC] 69698/01, para 103, ECHR 2007-V).

130 *Tshabalala-Msimang* (n 100) para 46.

The content, form and consequences of the publication may also be considered. In other words, the way in which the photo or report is published, the manner in which the person concerned is represented, and the ultimate effect of the publication should be taken into consideration.¹³¹ In the Instagram case, the European Court found that the risk of harm posed by content and communications on the internet to the exercise of the right to privacy certainly is higher than that posed by the press¹³² since the altered picture along with the caption had been accessible not only to X's followers on Instagram, but to other users of this platform.¹³³ Thus, decision-makers need to consider whether online newspapers should be under a requirement to notify subjects of stories which contain private information in advance.¹³⁴

Finally, the severity of the sanctions imposed is also a factor to be considered when assessing the proportionality of interference with the exercise of the freedom of expression.¹³⁵ This means the sanctions imposed to vindicate the right to privacy should not shackle the right to freedom of expression. For example, banning, impounding or interim injunctions might be imposed to defend the privacy of individuals, yet such measures may not disproportionately affect the press freedom of publishers and individuals. In the Axel Springer case, the European Court noted that the injunctions on publication of the photos accompanying the disputed articles could have a chilling effect on the applicant's company.¹³⁶ While the German regional Court imposed an injunction on the publication of the photos accompanying the disputed articles, such measures were capable of stifling the right to freedom of expression. It follows that an appropriate balance between the two rights must be placed. This implies that when the sanction imposed against the problematic publication is severe (largely to safeguard the right to privacy), it chills the right to freedom of expression. The next section turns to the second context of balancing the rights to freedom of expression and to privacy in the digital environment, i.e., the rights to be forgotten.

131 See *Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v Austria* (No 3) 66298/01 and 15653/02, para 47, 13 December 2005; *Reklos and Davourlis v Greece* 1234/05, para 42, 15 January 2009; and *Jokitaipale and Others v Finland* 43349/05, para 68, 6 April 2010.

132 *Delfi* (n 102) para 133.

133 *Einarsson* (n 114) para 46.

134 L Taylor 'Balancing the right to a private life and freedom of expression: Is pre-publication notification the way forward?' (2017) 9 *Journal of Media Law* 72-99.

135 *Pedersen and Baadsgaard v Denmark* [GC] 49017/99, ECHR 2004-XI, para 93.

136 *Axel Springer* (n 30) paras 108-109.

5 The right to be forgotten

The right to be forgotten is an emerging right of individuals that enables rights holders to rectify or correct personal data. The right to be forgotten has been discussed by the UN Human Rights Committee under General Comment 16 on the right to privacy.¹³⁷ In cases where individuals' private files maintained by public authorities contain incorrect personal data or have been collected or processed contrary to the provisions of the law, an individual should have the right to request rectification or elimination.¹³⁸

The right to be forgotten implies the right of rectification or erasure of data, which is addressed under the African human rights law such as the African Declaration. For example, a social media platform could retain information about individuals for the sake of imparting information. This, however, could jeopardise an individual's data privacy if the platform contains incorrect data about individuals. Additionally, African human rights law offers important normative provisions on the right to be forgotten.¹³⁹ For example, the African Union Cyber Convention on Security and Data Protection¹⁴⁰ under article 19 protects the right to be forgotten. The Convention stipulates:

Any natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, the personal data concerning him/her where such data are inaccurate, equivocal or out of date, whose collection, use, disclosure or storage are prohibited.

On the other hand, RECs have contributed to the development of data protection in Africa at the sub-regional level. Africa has eight RECs but only two as yet are significant in terms of the data privacy context, including the right to be forgotten: ECOWAS and SADC. The ECOWAS Supplementary Act spells out the right to rectify or destroy personal information, otherwise known as the right to be forgotten. The Act stipulates:

137 UN Human Rights Committee (HRC) CCPR General Comment 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988 para 10.

138 General Comment 16 (n 137) para 10.

139 LA Abdulrauf and CM Fombad, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?' (2016) 8(1) *Journal of Media Law* 67,85.

140 The Malabo Convention (n 69).

If personal data of which an individual is the data subject are inaccurate, incomplete, questionable, outdated or prohibited from collection, use, disclosure or preservation, [one] is entitled to ask the data controller to have such data rectified, supplemented, updated, blocked or destroyed, as appropriate.¹⁴¹

Accordingly, the data subject shall have the right to obtain from the controller the erasure of personal data where the data is for example prohibited. The SADC Model Law, on the other hand, envisages the right to be forgotten, which further invigorates data subjects to enforce their right to privacy on the internet from search engines and internet intermediaries.¹⁴² The Model Law is, however, not binding; instead, it serves as a template for SADC member states to enact domestic legislation on data protection. While some RECs - such as the ECOWAS and SADC - go further in incorporating specific data protection rules, including the right to be forgotten, there is, as yet, a dearth in jurisprudence concerning the enforcement of the right to be forgotten and the right to privacy before tribunals established at the sub-regional level.

By the same token, the African Declaration states that individuals have the right to be forgotten¹⁴³ in generic terms. Specifically, they have the right to erase personal information that is prohibited from collection, use, disclosure or storage. Despite these nascent normative rules, African states are yet to make compelling judicial pronouncements on how to balance the right to privacy and freedom of expression in the context of the right to be forgotten.

Balancing in the context of the right to be forgotten has arisen for discussion because the internet removes individuals' ability to live down their pasts.¹⁴⁴ Accordingly, the right to be forgotten may refer to the right to erasure,¹⁴⁵ forgetting, delisting and takedown.¹⁴⁶ In *Google Spain SL v*

141 Art 41 ECOWAS Act.

142 Art 32(1)(a) SADC Model Law.

143 African Declaration Principle 42(3)(d).

144 P Lambert 'The right to be forgotten: Context and the problem of time' (2019) 24 *Communications Law* 74-79. See S Kulk & FZ Borgesius 'Privacy, freedom of expression, and the right to be forgotten in Europe' in E Selinger and others (eds) *The Cambridge handbook of consumer privacy* (2018) 301-320.

145 Art 17 *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

146 C Bartolini & L Siry 'The right to be forgotten in the light of the consent of the data

*Agencia Española de Protección de Datos*¹⁴⁷ (*Google Spain* case) Mr González made a complaint to the Spanish Data Protection Agency (AEPD) against La Vanguardia newspaper, Google Spain and Google Inc, wanting the newspaper to remove or alter the record of his 1998 garnishment proceedings so that the information would no longer be available on the internet.¹⁴⁸ This matter was referred to the Court of Justice of the European Union (CJEU) to strike a balance between an individual's privacy and the public's access to information. The CJEU held that individuals whose personal data are publicly available through internet search engines may request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results.¹⁴⁹ The court in particular held:

their rights to privacy override not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.¹⁵⁰

However, the Court highlighted some the factors on which the balance may depend, namely, the nature of the information, its sensitivity for the data subject's private life and the interest of the public in having that information, an interest that may vary, in particular, according to the role played by the data subject in public life.¹⁵¹

Once a search engine operator like Google delists a search result, the right to freedom of expression could be triggered otherwise impinged in at least three ways.¹⁵² First, publishers' or journalists' freedom of expression would be muzzled since the publication or source will no longer be available. Second, search engine users have a right to receive information.¹⁵³ Third, a search engine operator exercises its freedom of expression when it offers its search results, which search results could be considered a form of expression.¹⁵⁴ As a result, search engine operators need to be cautious, and take competing interests seriously.

subject' (2016) 32(2) *Computer Law and Security Review* 218.

147 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos* 13 May 2014, Judgment, Case C-131/12, 13 May 2014, Court of Justice of the European Union [CJEU].

148 *Google Spain* (n 147) paras 14-15.

149 *Google Spain* (n 147) para 81.

150 As above.

151 As above.

152 See J van Hoboken *Search engine freedom: On the implications of the right to freedom of expression for the legal governance of web search engines* (2012) 350.

153 Kulk & Borgesius (n 144) 312.

154 Van Hoboken (n 152) 351.

In another landmark decision, the Grand Chamber of the CJEU in *Google LLC v French Data Protection Authority (CNIL)* ruled in favour of freedom of expression than privacy for extra-territorial balancing issues where the existing EU law did not oblige Google to carry out an order to de-reference search results on all versions of its search engine.¹⁵⁵ The right to be de-referenced (right to be forgotten) is geographically limited to EU member states.¹⁵⁶ Nevertheless, within the EU the right to privacy will be balanced against other fundamental rights, such as freedom of expression, in accordance with the principle of proportionality.¹⁵⁷

To conclude, following the *Google Spain* case, companies such as Google introduced commendable measures regarding the right to be forgotten, such as the preparation of an 'online form',¹⁵⁸ which enables applicants to request the delisting of particular results for searches on their name. When the request is being processed, Google must operationalise the balance between applicants' privacy with the public's interest to know and the right to freedom of expression.¹⁵⁹ The next section concludes.

6 Conclusion

Balancing the right to privacy against freedom of expression is an old question in the human rights law debate. However, the debate has resurfaced on the new domain: the internet. This chapter has demonstrated how balancing process provides a useful mechanism for reconciling the right to privacy and freedom of expression on the internet. What it requires is the identification, valuation, and comparison of competing rights. Yet, the balancing process remains an arduous task since courts in various jurisdictions have been grappling with offering an appropriate touchstone to balance the rights to privacy and to freedom of expression.

The African human rights law has sheer normative rules that could be used to resolve the issue of balancing the rights to privacy and freedom of expression. While there is no rich jurisprudence on balancing competing

155 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, The Grand Chamber of the Court of Justice of European Union (CJEU) 24 September 2019 para 72.

156 *Google LLC* (n 155) para 62.

157 *Google LLC* (n 155) para 60; *Volker und Markus Schecke and Eifert*, CJEU C-92/09 and C-93/09, EU:C:2010:662 para 48.

158 See Report content for legal reasons, Google, https://support.google.com/legal/answer/3110420?visit_id=637369736799701053-129110386&rd=2 (accessed 24 August 2023).

159 Removing Content from Google, <https://support.google.com/legal/troubleshooter/1114905?hl=en#ts=> (accessed 24 August 2023).

rights in the continent, the South African courts have resolved the balancing issues through applying the proportionality principle which is found under the limitation of rights clause in Section 36 of the Constitution.

To examine how the balancing exercise should be done, the chapter has explored two current contexts: the publication of personal information and an individual's right to be forgotten. First, in case of the publication of personal information where an individual's personal information is published on the internet, for example, the European Court has pointed out six-part touchstones, such as the contribution of personal information to the general debate; the method of obtaining the information; how the person concerned is well-known; the prior conduct of the person; the content, form and consequence of publication; and the severity of the sanctions to be imposed, which should be applied to balance the right to privacy and freedom of expression.

The chapter also discussed how the right to be forgotten is another context to strike a balance between the right to privacy and freedom of expression where the right holder requests the removal of online content where it is deemed unlawful as per Principle 42(3) of the 2019 African Declaration and Article 19 of the Malabo Convention. After the landmark Google Spain case in 2014, some internet intermediaries such as Google commenced an online form that could enable right holders to claim the right to be forgotten. For this reason, internet intermediaries and search engine operators should apply copious balancing touchstones as established by courts whenever they face balancing issues. Ultimately, as to which right prevails-whether the right to privacy or freedom of expression – the chapter argues that tipping the scale depends on several factors and should be addressed on a case-by-case basis.

Reference

- Abdulrauf, LA and Fombad, CM 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?' (2016) 8(1) *Journal of Media Law* 67
- Aleinikoff, TA 'Constitutional Law in the Age of Balancing' (1987) 96 *Yale Law Journal* 94
- Alexy, R 'Constitutional Rights, Balancing, and Rationality' (2003) 16 *Ratio Juris* 136
- Ayalew YE 'Assessing the limitations to freedom of expression on the internet in Ethiopia against the African Charter on Human and Peoples' Rights' (2020) 20 *African Human Rights Law Journal* 315
- Ayalew, YE 'Untrodden paths towards the right to privacy in the digital era under African human rights law,' (2022) 12 *International Data Privacy Law* 16
- Barendt, E 'Balancing freedom of expression and privacy: The jurisprudence of the Strasbourg Court,' (2009) 1 *Journal of Media Law* 49
- Barendt, E *Freedom of speech* (Oxford University Press, 2007)
- Barendt, E 'Privacy and freedom of speech' in AT Kenyon & M Richardson (eds) *New dimensions in privacy law: International and comparative perspectives* (Cambridge University Press 2006) 11-31
- Bartolini C and Siry, L 'The Right to Be Forgotten in the Light of the Consent of the Data Subject' (2016) 32(2) *Computer Law & Security Review* 218
- Bitew, A 'Social media and the simmering Ethiopian revolution' ECDAF (3 September 2016), <https://ecadforum.com/2016/09/03/social-media-and-the-simmering-ethiopian-revolution-alem-bitew/> (accessed 24 August 2023)
- Bomhoff, J *Balancing Constitutional Rights, The Origins and Meanings of Postwar Legal Discourse* (Cambridge University Press, 2013)
- Cali, B 'Balancing Human Rights - Methodological Problems with Weights, Scales and Proportions,' (2007) 29 *Human Rights Quarterly* 251
- Cannataci J and others 'Privacy, Free expression and Transparency and Redefining Their New Boundaries in the Internet Ecosystem' UNESCO Internet Study(2016)
- Cerf, VG 'Internet access is not a human right' *New York Times* (4 January 2012), <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html> (accessed 30 August 2023)

- Clarke, K & Kocak, K 'Launching revolution: Social media and the Egyptian uprising's first movers' (2020) 50(3) *British Journal of Political Science* 1025
- Dworkin, R 'Rights as Trumps' in Jeremy Waldron (ed), *Theories of Rights* (Oxford University Press, 1984)
- Dhillon, A 'Social media and revolution: The importance of the internet in Tunisia's uprising' (2014) *Independent Study Project (ISP) Collection* 1-21
- Dworkin, R *Taking rights seriously* (Harvard University Press, 1977)
- Erixon, F & Lee-Makiyama, H 'Digital authoritarianism: Human rights, geopolitics and commerce' European Centre for International Political Economy (ECIPE), ECIPE Occasional Paper 5/2011 (2011) 1, <http://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf> (accessed 24 August 2023)
- Fordham, M & de la Mare, T 'Identifying the principles of proportionality' in J Jowell & J Cooper (eds) *Understanding human rights principles* (2000) 31
- Gillespie, AA 'Restricting access to the internet by sex offenders (2011) 19 *International Journal of Law and Information Technology* 171
- Habermas, J *Between facts and norms* trans W Rehg (1996)
- Lambert, P 'The right to be forgotten: context and the problem of time' (2019) 24(2) *Communications Law*
- Loughlan, P, McDonald, B, Van Krieken, R *Celebrity and the law* (The Federation Press, 2010) 125
- Joyce, D Internet Freedom and Human Rights, (2015) 26 *European Journal of International Law* 493
- Joyce, D 'Privacy in the Digital Era: Human Rights Online?' (2015) 16 *Melbourne Journal of International Law* 1-15
- Koskeniemi, M *The politics of international law* (Bloomsbury Publishing, 2011) 144
- Land, M 'Toward an international law of the internet' (2013) 54 *Harvard International Law Journal* 393
- Lockwood, BB Finn, J & Jubinsky G 'Working Paper for the Committee of Experts on Limitation Provisions' (1985) 7 *Human Rights Quarterly* 35-88
- Mare, A 'Internet shutdowns in Africa: State-ordered internet shutdowns and digital authoritarianism in Zimbabwe' (2020) 14 *International Journal of Communication* 4244
- McGoldrick, D 'The limits of freedom of expression on Facebook and social networking sites: A UK perspective' (2013) 13 *Human Rights Law Review* 125

- Media Legal Defence Initiative (MLDI) 'Mapping digital rights and online freedom of expression in East, West and Southern Africa' (2018) 10-14, https://10years.mediadefence.org/wp-content/uploads/2019/07/Mapping-digital-rights-litigation_Media-Defence_Final.pdf (accessed 24 August 2023)
- Mendel, T and others *Global survey on internet privacy and freedom of expression* UNESCO Series on Internet Freedom, Paris: UNESCO (2012) 95
- Moosavian, RA 'Just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7 *Journal of Media Law* 196
- Murray, R *The African Charter on Human and Peoples' Rights a Commentary* (Oxford University Press, 2019)
- Mutua, M *Human rights: a political and cultural critique* (University of Pennsylvania Press, 2002)
- Mutua, M 'The Banjul Charter and the African cultural fingerprint: An evaluation of the language of duties' (1995a) 35 *Virginia Journal of International Law* 339
- Mutua, M 'Why redraw the map of Africa: A moral and legal inquiry' (1995b) 16 *Michigan Journal of International Law* 1146
- Nyirenda-Jere, T & T Biru 'Internet development and internet governance in Africa, Africa' (Internet Society, May 2015) 6
- Patricia, LP and others *Celebrity and the Law* (The Federation Press, 2010)
- Puddephatt, A *Freedom of expression and the internet* (UNESCO 2016)
- Rosenfeld, M & Arato, A *Habermas on law and democracy: Critical exchanges* (University of Carolina Press, 1998)
- Oxford Learners' Online Dictionary definition of the word 'balance' https://www.oxfordlearnersdictionaries.com/definition/english/balance_1?q=balance (accessed 24 August 2023)
- Raz, J *The morality of freedom* (Oxford University 1986) 166
- Singh, A & Power, M 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' (2019) 3 *African Human Rights Yearbook* 211
- Taha, N 'Sudan's social media deemed major player in Bashir's ouster' *VOA News* 18 April <https://www.voanews.com/a/sudan-s-social-media-deemed-major-player-in-bashir-s-ouster-/4882059.html> (accessed 24 August 2023)
- Taylor, L 'Balancing the right to a private life and freedom of expression: Is pre-publication notification the way forward?' (2017) 9 *Journal of Media Law* 72
- Tully, S 'A human right to access the internet? Problems and prospects' (2014) 14 *Human Rights Law Review* 180

van Hoboken, J *Search engine freedom: On the implications of the right to freedom of expression for the legal governance of web search engines* (2012) 350

Waldron, J 'Rights in Conflict,' (1989) 99 *Ethics* 503

PART II: Data privacy and artificial intelligence

4

THE ASCENT OF ARTIFICIAL INTELLIGENCE IN AFRICA: BRIDGING INNOVATION AND DATA PROTECTION

Emmanuel Salami

Abstract

Artificial intelligence (AI) systems have transcended science fiction and are now globally used in almost every facet of human endeavour. Whether in the development of AI to perform defined tasks or in the actual performance of said tasks by AI, AI systems process large volumes of big data (which includes both personal and non-personal data) with vast consequences for the right to data protection. In certain cases, AI systems can collect (personal) data from unsuspecting data subjects, resulting in vast proportions of data processing that are not usually anticipated with traditional technological devices. This potentially raises a plethora of data protection law concerns. The acknowledgment of the potential implications of AI within and outside the scope of data protection law has led to a massive production of literature from regulators and scholars around the world aimed towards the regulation and lawful use of AI. However, it appears that the regulation of AI by data protection law has yet to attract such momentum across the African continent. This is despite the fact that there is evidence of wide usage of AI systems across the continent. This is further worsened by the lack of (sufficient) data protection regulatory instruments across many African countries. At the continental level, member states have failed to ratify the African Union Convention on Cybersecurity and Personal Data Protection, thereby making it impossible for it to come into force. The result of this can only be a violation of the right to data protection of the residents of African countries by both indigenous and foreign actors who ironically respect the rights of data subjects in countries and regions having sufficient data protection laws. AI promises to automate a lot of processes ensuring vast technological advancements in its wake. However, violations of the right to data protection owing to the lack or insufficiency of data protection regulatory instruments threatens to rob Africa of the benefits of AI. Relying on selected continental, regional and national data protection regulatory instruments, this chapter assesses the impact of the usage of AI systems on the right to data protection across the African continent. Data protection concerns that arise from the use of AI will be identified and assessed in light of these selected African laws with appropriate recommendations being made where necessary. The research methods that are

used to achieve the objectives of this chapter include a comparative analysis between certain aspects of the selected 'African' data protection laws under review and the data protection laws in some other countries and/or regions. The doctrinal research method is also relied upon by analysing existing statutory (where applicable), judicial and scholarly documents on the data protection regulation of AI in Africa. As there is a dearth of African literature on this topic, the overarching objective of this chapter is to spur discussions about the data protection concerns inherent in the use of AI across the African continent which, in turn, will birth more legislative interest, scholarly research and, hopefully, genuine efforts at regulation.

1 Introduction

The proliferation of artificial intelligence (AI) has become a global phenomenon partly because of the automation and relative ease it brings to the execution of various activities, especially those that could otherwise be very challenging. Notable industries across the African continent have adopted AI in their day-to-day operations. Africa has a fragmented regulatory approach to data protection law despite the enactment of the African Union Convention on Cybersecurity and Personal Data Protection (AU Convention)¹ which has been largely overlooked by most member states of the African Union (AU).² It would appear that the global rejuvenation of data protection law regulation that became the norm after the entry into force of the General Data Protection Regulation (GDPR)³ has also had an impact across the continent with more African countries enacting data protection regulatory instruments after the entry into force of the GDPR.⁴ In other cases, a good number of African countries have left

- 1 African Union Convention on Cyber-Security and Personal Data Protection (27 July 2014) EX.CL/846(XXV).
- 2 Only fifteen out of a total of 55 member states of the AU have ratified the convention. See African Union 'List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security And Personal Data Protection' https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (accessed 10 March 2024).
- 3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (4 May 2016) OJ L119/1.
- 4 No less than eight African countries enacted data protection laws after the entry into force of the GDPR. These countries are Algeria (2018); Botswana (2018); Nigeria (2019); Uganda (2019); Kenya (2019); Congo-Brazzaville (Republic of Congo) (2019); Togo (2019); and Egypt (2020).

data protection law completely unregulated with varying consequences.⁵ There is the possibility that data protection regulatory instruments across the African continent may not be well suited for the regulation of AI, thereby necessitating law reform. The importance of this consideration lies in the fact that the deployment of AI ordinarily poses enormous data protection law concerns, and this ought to be remediated.⁶ It is arguable that limitations in technological advancements might have contributed to the selective lack of enthusiasm that bedevilled data protection law regulation across the continent.⁷ Another school of thought might also blame the continent's chequered history with fundamental human rights enforcement as a reason for the hesitation that has courted its approach to the regulation of data protection governance.⁸

As previously stated, AI poses data protection concerns of vast proportions due to some of the following capabilities of AI: personal data⁹ collection without the knowledge of data subjects; the collection of more personal data than ordinarily is necessary for the purpose of the processing activity;¹⁰ making conclusions and decisions that affect the fundamental rights and freedoms of data subjects; and so forth. Therefore, any absence of proper regulation threatens to greatly violate the rights (including the right to dignity) of data subjects.¹¹ One of the objectives of this chapter is to consider the data protection concerns that are naturally attendant to the

- 5 At the time of writing this chapter, there are 18 African countries where data protection law is unregulated. See G Greenleaf & C Bertil 'Comparing African data privacy laws: International, African and regional commitments' (22 April 2020) University of New South Wales Law Research Series, <https://ssrn.com/abstract=3582478> (accessed 15 September 2020).
- 6 Data subject means any identified or identifiable natural person that is the subject of personal data processing. See art 1 AU Convention; sec 2 Data Protection Act, 2019; Kenya Gazette Supplement 181 (Act 24) (DPAK); art 1 Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (adopted at the 37th session of the Authority of ECOWAS Heads of State and Government on 12 February 2010, Abuja, Nigeria) (ECOWAS Act).
- 7 Z Adaramola 'Why Africa is backward in technology – NOTAP' (21 June 2012), <https://allafrica.com/stories/201206210900.html#:~:text=The%20National%20Office%20for%20Technology,growth%20of%20technology%20in%20Africa> (accessed 14 September 2020).
- 8 Amnesty International 'Africa 2019' (Amnesty.org), <https://www.amnesty.org/en/countries/africa/report-africa/> (accessed 10 September 2020).
- 9 Personal data means any information relating to an identified or identifiable natural person. Art 1 AU Convention; art 1 ECOWAS Act; sec 2 Data Protection Act of Kenya (DPAK).
- 10 Data processing is any operation carried out on personal data. See art 1 AU Convention; sec 2 DPAK.
- 11 European Union Agency for Fundamental Rights and the Council of Europe *Handbook on European data protection law* (2018) 19.

ascent of AI in Africa. The risks posed by these concerns are assessed in light of the efficacy of applicable data protection laws to mitigate identified risks. Since there is no uniform African data protection law, these concerns will be considered on the basis of selected continental, regional and national data protection laws. For this purpose, the AU Convention, the Economic Community of West African States Supplementary Act on the Protection of Personal Data (ECOWAS Act),¹² and the Data Protection Act of Kenya 2019 (DPAK) will be used to gauge the level of compliance across the continent.¹³ These laws will collectively be referred to as the ‘focus legislations’. The AU adopted the AU Convention in 2014 and it requires 15 signatories to come into force.¹⁴ It got the fifteenth signature in April 2023.¹⁵ In respect of the ECOWAS Act, the 15 member states of ECOWAS are bound by this Act and are obliged to adopt their own data protection laws.¹⁶ In November 2019 Kenya passed its Data Protection Act into law making it the country’s first data protection legislation.

Irrespective of the enforceability or effectiveness of these laws, they represent a selective overview of data protection law(s) across the continent and are considered herein for this purpose. This study considers these legislations because of their status as leading legislation at the continental, regional, and national levels. The Data Protection Act of Kenya has been particularly selected because of its adoption of internationally accepted data protection standards, making it a model African data protection legislation. The consideration of these regulatory instruments is limited to their role in achieving data protection compliance in the use of AI.

As far as possible, reference will only be made to actual deployments of AI across the African continent to ensure that the considerations herein are genuinely Afrocentric. This chapter is divided into six parts aimed at fully addressing relevant issues under consideration. Part 2

12 Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (adopted at the 37th session of the Authority of ECOWAS Heads of State and Government, 12 February 2010, Abuja, Nigeria).

13 Data Protection Act, 2019, Kenya Gazette Supplement 181 (Act 24).

14 Art 36 AU Convention.

15 Mauritania recent ratification made it the 15th ratification required to come into force. So far, only Angola, Cape Verde, Côte d’Ivoire, Congo, Ghana, Guinea, Mauritius, Mauritania, Mozambique Namibia, Niger, Rwanda, Senegal, Togo and Zambia have ratified the AU Convention. Thirteen other countries (Benin, Cameroon, Chad, Comoros, Congo-Brazzaville, Djibouti, Gambia, Guinea-Bissau, South Africa, Sierra Leone, Sao Tome & Principe, Sudan and Tunisia) have signed but not ratified it.

16 Arts 47 & 48 of the ECOWAS Act. See ECOWAS Revised Treaty of the Economic Community of West African States (ECOWAS) (24 July 1993). See also ECOWAS ‘ECOWAS Law – Treaty’, <https://www.ecowas.int/ecowas-law/treaties/> (accessed 10 September 2020).

defines relevant concepts and terms such as AI, machine learning big data, and so forth. The instances of practical deployments of AI as well as the data protection concerns and applicable remediation actions in the use of AI in Africa are addressed in parts 3 and 4 respectively. Part 5 addresses the possible consequences of inadequate data protection legislations across the continent. This chapter concludes by assessing the above considerations and summarising the necessary steps for improving AI-specific data protection compliance in Africa. Some relevant concepts that are fundamental to this topic are subsequently considered.

2 An overview of relevant concepts

Although there is no consensus definition of AI, a perusal of scholarly literature would reveal some common conceptual attributes that cut across various definitions. This chapter will abstain from considering the definitional problems of AI and will rather focus on referencing some valuable definitions for the purpose of retaining a working definition for the purpose of this chapter. McCarthy, an AI pioneer credited with coining the term AI,¹⁷ defined AI as the science and engineering of making intelligent machines, especially intelligent computer programmes. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.¹⁸ Turing is another pioneer who designed what now is known as the Turing test used for determining the intelligence of machines.¹⁹ According to Turing, a machine is to be considered intelligent if it could successfully pretend to be human to a knowledgeable observer.²⁰ Russel and Norvig define AI as ‘the study of agents that exist in an environment and perceive and act’.²¹ One common thread running through these definitions is the indication that AI systems are designed to simulate human intelligence even though, as McCarthy notes, machines can be trained by making them study ‘problems the world presents to intelligence’ rather than studying human beings.²² AI can also be classified

17 P Stone and others ‘Artificial intelligence and life In 2030: Report of the 2015-2016 Study Panel’ (September 2016), https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf (accessed 10 September 2020).

18 J McCarthy ‘What is artificial intelligence?’ (12 November 2007) 2-3, <http://jmc.stanford.edu/articles/whatisai.html> (accessed 10 September 2020).

19 AM Turing ‘Computing machinery and intelligence’ (1950) 433-460, <https://www.csee.umbc.edu/courses/471/papers/turing.pdf> (accessed 24 August 2020).

20 As above.

21 SJ Russell & P Norvig *Artificial intelligence: A modern approach* (2010) 7.

22 McCarthy (n 18) 2.

into strong AI²³ and weak AI.²⁴ As of today, weak AI is more prevalent as AI systems are mostly able to perform particular tasks with human input.

‘Machine learning’ is a type of AI that provides computers with the ability to learn without being explicitly programmed to perform relevant tasks.²⁵ Machine learning has also been defined as the use of algorithms²⁶ to analyse data with the aim of discovering useful patterns (relationships or correlations) that can be used to make inferences.²⁷ Machine learning is used to detect patterns in data in order to automate complex tasks or make predictions.²⁸ In lay terms, machine learning is used to detect patterns in data in order to automate complex tasks and/or make predictions. Another significant concept is ‘big data’ which is indispensable to the functioning of AI. This is partly because machine learning is only possible with the use of big data without which it will be impossible for AI to automate tasks or identify patterns. The term ‘big data’ is also not short of divergence in definition.²⁹ A widely-used definition of big data is ‘3Vs definition’ which defines it as high volume, high velocity and high variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.³⁰ Based on this definition, it can be said that big data are large volumes of data that cannot be processed through the traditional methods of processing data. Having considered

- 23 Strong AI can perform unfamiliar tasks as it is equipped with comprehensive knowledge and cognitive capabilities ensuring that it has enough intelligence to solve problems. See I Bello ‘Beginners’ guide to artificial intelligence (AI)’ (17 July 17 2017), <https://becominghuman.ai/beginners-guide-to-artificial-intelligence-ai-ec8a409b6424> (accessed 13 October 2020).
- 24 Weak AI performs particular tasks with varying levels of human input. See Bello (n 23).
- 25 M Rouse ‘What is machine learning’, <https://whatis.techtarget.com/definition/machine-learning-algorithm> (accessed 24 August 2020).
- 26 An algorithm is an unambiguous procedure to solve a problem or a class of problems. It typically is composed of a set of instructions or rules that take some input data and return outputs. See C Castelluccia & D le Métayer ‘Understanding algorithmic decision-making: Opportunities and challenges’ European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261 (March 2019), [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU\(2019\)624261_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf) (accessed 7 September 2020).
- 27 S Finlay *Artificial intelligence and machine learning for business. A no-nonsense guide to data driven technologies* (2018) 6.
- 28 DE Sorkin ‘Technical and legal approaches to unsolicited electronic mail’ (2001) 35 *University of San Francisco Law Review* 325, 326.
- 29 See D Boyd & K Crawford ‘Six provocations for big data’ A decade in internet time: Symposium on the Dynamics of the Internet and Society, (September 2011) 1, <https://ssrn.com/abstract=1926431> (accessed 6 September 2020).
- 30 Gartner IT glossary ‘Big data’, <http://andandwww.gartner.comandit-glossaryandbig-data> (accessed 7 September 2020).

the definition(s) of these relevant concepts, examples of the usage of AI in Africa are subsequently considered.

3 Actual deployments of artificial intelligence in Africa

A consideration of the actual deployment of AI in Africa aids the appreciation of the fact that AI now is an African reality that requires legislative attention and is not merely another academic discourse. This consideration will also aid an understanding of the concerns that might be posed by AI in the context of its application in Africa. Some existing deployments of AI across Africa are listed as follows:

AI system/Developer	Industry	Processing activity
Sophie Bot	Health care	This chatbot serves as a platform for young persons in Kenya to obtain information on sexual and reproductive health. ³¹
SyeComp	Agriculture	SyeComp processes geospatial data from satellites and drone sensors for monitoring farms. ³²
DataProphet	Finance	DataProphet uses machine learning techniques for predictive analytics in conversation agents in South Africa. ³³

31 <https://www.f6s.com/sophiebot> (accessed 7 September 2020); C Harrington 'Improving access to sexual health education in Kenya with artificial intelligence' (15 January 2020) Humans of Machine Learning.

32 <https://syecomp.com/> (accessed 7 September 2020).

33 <https://dataprophet.com/de/> (accessed 7 September 2020).

Numberboost	Health care	Numberboost developed an AI system that supports mobile HIV clinics which provide medical access and services to different rural South African communities. Numberboost manages the scheduling and communication channels for patients seeking answers to sensitive medical questions. ³⁴
AI-based drones	Health care, product delivery, etc	AI-based drones are being used across the continent for various purposes which include the delivery of products to data subjects. In Rwanda for instance, drones are used to deliver critical medical supplies to hospitals and medical centers. ³⁵

34 <https://www.numberboost.com/>(accessed 7 September 2020).

35 JW Rosen ‘Zipline’s ambitious medical drone delivery in Africa’ MIT Tech Review (8 June 2017), <https://www.technologyreview.com/2017/06/08/151339/blood-from-the-sky-ziplines-ambitious-medical-drone-delivery-in-africa/> (accessed 7 September 2020).

Robots	Health care, service delivery, medical assistance, elder care, mining, etc.	Robots have been adopted in various African countries to provide support in various sectors of the African life and economy. A very popular example of this is the deployment of robots across the continent to provide support services at hospitals, ³⁶ airports, ³⁷ and universities, ³⁸ as a response to the outbreak of the COVID-19 pandemic.
--------	---	--

The deployment of AI across Africa is also visible in the finance sector where AI is being used for various purposes, including determining loan eligibility. There also is the opportunity for the futuristic deployment of autonomous cars in Africa even though as Africa's infrastructural reality suggests, this might not be happening any time soon.³⁹

4 How do artificial intelligence systems collect (personal) data?

In order to enhance the comprehension of the relevant issues that are identified herein, it is important to identify some of the avenues through which AI collects (personal) data. AI systems typically collect large volumes of big data that which includes both personal and non-personal

36 D Miriri 'Rwandan medical workers deploy robots to minimise coronavirus risk' World Economic Forum (5 June 2020), <https://www.weforum.org/agenda/2020/06/rwandan-medical-workers-robots-coronavirus-covid19-risk/> (accessed 7 September 2020).

37 A Odutola 'FG acquires profiling robots for airport' Nairametrics (27 June 2020), <https://nairametrics.com/2020/06/27/fg-acquires-profiling-robots-at-airport/> (accessed 7 September 2020).

38 'Unilag gets robots for temperature, blood pressure checks' Vanguard (29 June 2020), <https://www.vanguardngr.com/2020/06/covid-19-unilag-gets-robots-for-temperature-blood-pressure-checks-others/> (accessed 7 September 2020).

39 S Malinga 'SA not ready for autonomous vehicles' ITWeb (7 October 2020), <https://www.itweb.co.za/content/kYbe97XxPyQ7AWpG> (accessed 7 September 2020).

data. It is the personal data collected by AI that forms the crux of this chapter. The data collection avenues identified in this part reflect some of the channels through which some of the AI systems stated above collect (personal) data. These avenues are identified in the paragraphs below.

One of the avenues for data collection in AI systems is through computer vision, which equips AI with the ability to 'see' and allows images or videos to be analysed using machine learning algorithms. Large volumes of (personal) data can be generated daily from AI systems using computer vision. These large volumes of (personal) data can be processed to provide insights capable of automating various systems and processes.⁴⁰ AI systems that are able to 'see' their environments, identify objects, scan documents, and so forth, are able to do this through the use of computer vision. In viewing its environment, AI systems designed with computer vision are able to capture large volumes of human images, buildings, vehicle plate numbers, and so forth, which, when combined with other data, might lead to the identification of natural persons. Computer vision has been used for a while in some popular applications, which include facial recognition, image classification, visual sensors, image search, photograph restoration, industrial robotics, autonomous vehicles, cancer detection, and so forth.⁴¹ Computer vision uses specialised types of neural nets known as convolutional neural nets to build models of objects from a large collection of examples.⁴²

AI collects large volumes of (personal) data collected through sensors that identify objects, persons, road users, and so forth. Most computer vision systems rely on image sensors. Some examples of sensors are lidar which uses lights to scan over a distance of 100 metres in all directions;⁴³ radar which uses radio waves to determine the speed, distance and angle of moving objects;⁴⁴ camera, which is the most popular sensor and is very effective for scene interpretation; ultrasound measures the distance between objects using sound waves.⁴⁵ Speech recognition technology is another avenue for data collection in AI. It allows users to interact with

40 J Tay and others 'Application of computer vision in the construction industry' (19 November 2019), <https://ssrn.com/abstract=3487394> (accessed 7 September 2020).

41 N Malik & PV Singh 'Deep learning in computer vision: Methods, interpretation, causation and fairness', (28 May 2019), <https://ssrn.com/abstract=3395476> (accessed 7 September 2020).

42 J Kaplan *Artificial intelligence: What everyone needs to know* (2016) 54.

43 A Herrmann, W Brenner & R Stadler *Autonomous driving: How the driverless revolution will change the world* (2018) 95.

44 Herrmann and others (n 44) 95-96.

45 As above.

AI by singling out their words or phrases in a specific language and thereafter converting it to a machine-readable format.⁴⁶ Mainstream usages of this technology can be found in Google Voice, Amazon's Alexa, Microsoft's Cortana, and Apple's Siri.⁴⁷ Other means of data collection include the use of data supplied into chatbots by its users, processing of anonymised⁴⁸ customer data for machine-learning purposes, and so forth.

5 Data protection concerns and remedies in the deployment of artificial intelligence in Africa

In the processing of large volumes of big data, AI systems also process the personal data of data subjects. The peculiarities of AI systems mean that said processing activities raise various concerns in the context of the right to data protection of data subjects. These concerns are assessed within the scope of the focus legislations with the aim of discovering how effective these laws are in resolving identified challenges. Recommendations aimed at the resolution of identified concerns are also considered. These concerns are identified as follows:

5.1 Lawfulness principle

The requirement that personal data should be processed lawfully embodies a foundational and fundamental principle of data protection law. This principle generally requires that the processing of personal data should be grounded in one of the recognised legal bases for processing personal data under data protection law.⁴⁹ This principle is reflected in the focus legislations as follows:

Article 13 (Principle 1) of the AU Convention provides, among others, that personal data shall be processed legitimately where data subjects have given their consent or also processed alternatively on the basis of a legal obligation; the performance of a task in the public interest or in the exercise of official authority vested in the controller or in a third party; for the performance of a contract to which the data subject is party or in order to

46 Kaplan (n 43) 57-60.

47 N van der Velde 'Speech recognition technology overview' Globalme Language and Technology (8 July 2019), <https://www.globalme.net/blog/the-present-future-of-speech-recognition/> (accessed 7 September 2020).

48 Anonymised data is data that does not lead to the identification of natural persons because it has been deidentified and as a result does not fall within the scope of data protection law. See sec 2 DPAK.

49 Art 5 GDPR. See P Carey *Data protection: A practical guide to UK and EU law* (2018) 33. See also LA Bygrave 'Data protection law: Approaching its rationale, logic and limits' (2002) 10 *Information Law Series* 58.

take steps at the request of the data subject prior to entering into a contract; to protect the vital interests or fundamental rights and freedoms of the data subject. From this provision of the AU Convention, two apparent points come to mind: The AU Convention appears to make consent a primary legal basis, the use of which may only be derogated from where there are alternative legal bases that may be relied upon and 'legitimate interest of the controller' as a justifiable legal basis is omitted under said Convention.⁵⁰ Article 23 of the ECOWAS Act lists consent; compliance with a legal obligation; public interest of a public authority; performance of a contract or for the application of pre-contractual measures adopted at the data subject's request; for safeguarding the interests or rights and fundamental liberties of the data subject as legal bases for processing personal data. Section 25(b) of DPAK provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to any data subject. Section 30(1) of DPAK further provides that personal data shall only be processed on the basis of consent, the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; for compliance with any legal obligation to which the controller is subject; in order to protect the vital interests of the data subject or another natural person; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the performance of any task carried out by a public authority; for the exercise of functions in the public interest; for the legitimate interests pursued by the data controller or other party to whom the data is disclosed and for the purpose of historical, statistical, journalistic, literature and art or scientific research.

One concern that pertains to the lawfulness principle is the determination of an appropriate legal basis for the processing activities of AI systems. In the use of AI, the most probable legal basis for conducting processing activities is the consent of the data subject or the performance of a contract. However, these can only be relied upon where personal data is collected from data subjects who are actively transacting with data controllers. The nature of AI systems that capture observed data,⁵¹

50 See art 6(1)(f) GDPR that provides for the use of 'legitimate interest of the controller' as a legal basis. The nature of this legal basis has been considered by the now defunct Article 29 Data Protection Working Party (A29WP). See A29WP Opinion 06/2014 on the 'Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP217 (9 April 2014).

51 Observed data is recorded automatically from data subjects even though they may be unaware of this in some cases. Interestingly, observed data can lead to the identification of other categories of personal data about a natural person. Eg, from a person's picture, their religious orientation (eg through the use of the hijab), race, political affiliations (through the inscriptions on clothing) etc might be deductible, thereby making observed data critical in the protection of personal data. For further readings on the

such as images of unsuspecting pedestrians and bystanders, renders the application of these legal bases legally impossible.⁵² It suffices to say that innocent pedestrians and bystanders can neither be said to have consented to the collection of their personal data nor to have entered into a contract with data controllers. While 'legitimate interest' may appear like a possible legal basis, the balancing test that ought to be conducted before the said legal basis can be relied upon might suggest that the legitimate interest of the controller may not outweigh the fundamental rights and freedoms of data subjects, particularly pedestrians and passers-by who are unaware of any data collection.⁵³ Irrespective of this consideration, the use of legitimate interest as a legal basis will be inapplicable under the AU Convention as it is silent on said legal basis.

The nature of other possible legal bases, such as 'legal obligation', 'public interest' and 'vital interest', particularly in non-public sector processing activities, clearly makes these inapplicable in the context of this consideration.⁵⁴ Based on the above assessment, the focus legislations are not particularly suited for the processing of observed personal data.

To resolve this concern, it is necessary to revisit the data collection procedures of AI. The identified problems that may emanate from the lack of a sufficient legal basis for processing personal data may largely be avoided if data collection is directed only to data subjects that are transacting in one way or the other with data controllers. However, in some cases this recommendation may not always be feasible. For instance, in the use of autonomous cars, personal data, including IP addresses, images, and so forth, will be collected from both pedestrians and passers-by for reasons that include the prevention of accidents and mishaps.⁵⁵ Due to the fundamental purpose sought to be achieved by these processing activities, it might be necessary that laws be amended to define and justify

classification of data, see The Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' (4 September 2017) 12-13.

52 This very concern is related to the data minimisation principle and will be subsequently addressed.

53 For further readings on the necessity and nature of the 'balancing test', see Information Commissioner's Office 'Legitimate interest: At a glance', <https://andandico.org.uk/andfor-organisationsandguide-to-the-general-data-protection-regulation-gdprandlawful-basis-for-processingandlegitimate-interestsand/> (accessed 23 November 2018); Opinion of the Article 29 Working Party: Opinion 06/2014 on the notion of legitimate interests of the data Controller under Article 7 of Directive 95/6/EC.

54 For further readings on applicable legal bases for processing personal data, see Carey (n 50) 50-54.

55 L Sweeney 'Matching known patients to health records in Washington State data' (5 June 2013), <https://ssrn.com/abstract=2289850> (accessed 26 September 2020).

these measures towards data collection, thereby making ‘legal obligation’ a justifiable legal basis for this purpose.⁵⁶ In some cases personal data might be anonymized, thereby making data protection law inapplicable. However, technological advancements mean that anonymised data may be reidentifiable in a way that leads to the identification of natural persons, thereby making personal data applicable.⁵⁷ Before personal data is treated as truly anonymised, adequate measures aimed at the prevention of data reidentification must be taken into consideration. Irrespective of the legal basis sought to be used in any processing activity, data subjects must be made fully aware of the ramifications of the processing activity especially because of the ability of AI to generate personal data from even the most innocuous of data categories.⁵⁸ This necessity of adequate information forms a key link to the transparency principle, which is addressed in the succeeding paragraph.

5.2 Transparent processing of personal data

Another principle of data protection that is relevant in the use of AI is the transparency principle that requires that data subjects should be provided with adequate information about the processing activity.⁵⁹ By virtue of this principle, data subjects should be provided with this right at the point of data collection. This principle is also important as it helps data subjects to pursue the enforcement of their data subject rights under any processing activity because the enforcement of such rights can only be achieved when data subjects are aware of the facts of the processing activity.⁶⁰ In practice, it is typical to provide data subjects with information about a processing activity through signposts, notice boards, privacy policies, and so forth.

56 E Salami ‘Autonomous transport vehicles versus the principles of data protection law: Is compatibility really an impossibility?’ (2020) *International Data Privacy Law Journal*, <https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipaa017/6007987> (accessed 2 December 2020).

57 K Bode ‘Researchers find “anonymised” data is even less anonymous than we thought’ Motherboard (3 February 2020), https://www.vice.com/en_us/article/dygy8k/researchers-find-anonymised-data-is-even-less-anonymous-than-we-thought (accessed 26 August 2020).

58 Researchers have been able to identify the right driver from 15 minutes’ worth of data from brake pedal use. See M Enev and others ‘Automobile driver fingerprinting’ (2016) (1) *Proceedings on Privacy Enhancing Technologies* 34-50, doi: <https://doi.org/10.1515/popets-2015-0029>.

59 Arts 5(1) and 13 GDPR. See Carey (n 49) 42. See also H Jackson ‘Information provision obligations’ in E Ustaran (ed) *European data protection law and practice* (2018) 169-193.

60 Art 29 Working Party Guidelines on transparency under Regulation 2016/679, adopted 29 November 2017, 17/EN WP260 rev.01, as last revised and adopted on 11 April 2018.

This principle is reflected in the focus legislations as follows: Article 13(5) of the AU Convention makes it mandatory for data controllers to disclose information on personal data. Article 27 of the ECOWAS Act requires data controllers to provide information about the processing of personal data. Section 25(b) of DPAK provides, among others, that data controllers and processors should process personal data transparently in relation to any data subject. The focus legislations are silent on what information is to be provided,⁶¹ the manner in which the information is to be provided,⁶² and at what point in the processing activity the information is to be provided to data subjects.⁶³ It is typical and rational to provide such information to data subjects before or at least at the time of data collection as this will help them exercise their rights, for example, to object to the processing of their personal data. In the use of AI, the provision of data subjects with information about the processing activity when there is a subsisting processing activity with the data controller may not be a grave concern even though it remains to be seen if said information will be provided timeously, that is, before or at the time of personal data collection. In cases where observed personal data is collected from pedestrians and passers-by, this also poses concerns in the context of the transparency principle because of the difficulty of providing such information to data subjects. In some cases, particularly in the use of closed-circuit television (CCTV) cameras, video surveillance and facial recognition by law enforcement agents, it is typical to use signposts and notice boards to provide adequate information to the data subjects about the relevant processing activity. This method also provides data subject with information at the point of data collection. In an African context, some of the AI systems being developed are focused on providing rural dwellers with easy access to social services. Traditionally, African rural communities have established methods and channels of communication.⁶⁴ It might be a more effective approach if these established rural communication methods and channels for making relevant AI-related communications to rural dwellers are used where feasible. It is acknowledged that some of these methods and channels of communication might have become counterproductive in light of modern

61 Typically, data protection legislations specify information such as the name of the controller, name of the processor, retention periods, etc as some of the information that ought to be provided to data subjects. See art 13 GDPR.

62 See Recital 58 and art 12 GDPR. See also art 29 Working Party (n 60) 7-10.

63 Eg, art 13(1) of GDPR provides among others that data subjects are to be provided with information about their processing activity 'at the time when the personal data are obtained'. See also art 29 Working Party (n 60) 14-16.

64 Traditional media of communication as tools for effective rural development (iproject), <https://iproject.com.ng/mass-communication/traditional-media-of-communication-as-tools-for-effective-rural-development-4257/index.html> (accessed 22 September 2020).

technology. However, technologies that adopt the mode of communication of traditional systems might also be helpful if developed and adopted in rural communities. For instance, ‘robot town criers’,⁶⁵ fluent in the native language of the rural community and stationed at strategic places such as open markets, which can be programmed to disseminate information at strategic times, might be an effective way of providing rural dwellers with relevant information about the use of AI. This recommendation is even more effective for those communities lacking in electricity, connection to media houses, and so forth. Town hall meetings, sensitisations through media outfits such as radio and television stations, newspaper adverts, and so forth, may also be an effective means of providing relevant information. In the Google street view case of *EDÖB v Google* the Swiss Federal Supreme Court held (among other things) that in Google’s collection of personal data, notice ought to be provided to data subjects in both the local and regional media.⁶⁶ To avoid selective application, it might be beneficial for regulators to specifically outline a minimum list of information that should be provided to data subjects in a processing activity.

5.3 Purpose limitation

In the processing of personal data, data controllers are required to specify and make the purpose of the processing activity explicit. This principle also requires that personal data should not be processed in a manner that is incompatible with the purpose for which they were initially collected.⁶⁷ This principle is reflected in the focus legislations as follows: Article 13(3)(a) of the AU Convention provides that data shall be collected for specific, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. Article 25(1) of the ECOWAS Act provides that personal data shall be obtained for specified, explicit, and lawful purposes and shall not be further processed in any manner incompatible with such purposes. Section 25(c) of DPAK provides that personal data shall be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

However, in the use of AI, machine learning generates new insights about data, which prompts data controllers to initiate new purposes for

65 Town criers serve as the traditional communication link between the village ruler(s) and the general village populace. See DSM Koroma ‘Traditional forms of communication of the Malimba of Sierra Leone’ (2018) 10, <http://unimak.edu.sl/wordpress/wp-content/uploads/MALIMBA-PROF-KOROMA.pdf> (accessed 22 September 2020).

66 BGE 138 II 346.

67 Art 5(1)(b) GDPR. See also Carey (n 49) 34; Bygrave (n 49) 61.

processing personal data a process known as data repurposing.⁶⁸ In such cases the legal basis and related considerations upon which the initial processing activity was carried out will not apply to the new processing activity because the processing activity did not form part of the purposes for processing personal data at the time of data collection.⁶⁹ However, it is clear that these provisions forbid further processing of personal data in a manner that is incompatible with the purposes for which it was initially collected. In practice, the provisions of the focus legislations are vague, particularly in the context of the provision restricting 'further processing of personal data in a manner that is incompatible with its initial purpose'. Therefore, the focus legislations are silent on the considerations necessary for the further data processing or repurposing of personal data in relation to the lawfulness principle. The factors to be considered in determining whether a new purpose of data processing incompatible with the initial purpose of processing are not outlined in the focus legislations and this could pose concerns in processing activities carried out by AI systems. This concern is even more amplified when the increased chances for data repurposing in AI systems are considered.

The regulatory approaches depicted in the relevant provisions of the focus legislations is distinguishable from article 6(4) of GDPR which provides, among others, conditions such as the relationship between the data controller and the data subject; the context of data collection; the possible consequences of increased processing on data subjects; and so forth. These conditions can then form the basis of an assessment for the purpose of revisiting the conditions for further processing in AI systems. Therefore, it is necessary for regulators to provide the necessary guidance which can help define the conditions that will justify further processing of personal data by AI systems. As the focus legislations are, there is much room for selective and subjective application of the rules for

68 AI processes large volumes of big data with a high tendency to discover new purposes of processing that were not envisaged at the commencement of the processing activity. For further readings, see R Pierce 'Machine learning for diagnosis and treatment: Gymnastics for the GDPR' (2018) 4 *EDPL* 339-340. See also M Shacklett 'Repurpose big data to get more analytics bang for your bucks' (28 January 2014), <https://www.techrepublic.com/article/repurpose-big-data-to-get-more-analytics-bang-for-your-bucks/> (accessed 12 September 2020).

69 This principle can be further appreciated when one considers the fact that assuming a privacy impact assessment was carried out before the commencement of the processing activity, such privacy impact assessment will not have taken that new purpose into perspective, thereby exposing the processing activity to unforeseen risks.

further processing of personal data and this might potentially result in the violation of the right to data protection.

5.4 Algorithmic bias and decision-making artificial intelligence systems

Research has found that while the source of algorithmic bias⁷⁰ in AI systems may remain unclear, said algorithmic bias may have two prominent root causes. The first possible root cause emanates from the use of biased and non-representative training data at the machine-learning phase. The second possible root cause is the development of the algorithms behind relevant AI systems by biased and/or non-representative engineers.⁷¹ Non-representative training data would be any data that does not truly represent all those that will be potentially subject to an AI system. Erroneous, unfair and unfounded inferences, predictions, conclusions, and decisions about data subjects are typically the end result of algorithmic bias. Once algorithms are biased, AI-based decisions are usually discriminatory and prejudicial against the group of people (typically minorities) who are underrepresented in the training data, thereby negatively affecting their fundamental rights and freedoms. Article 28 of the African Charter on Human and Peoples' Rights (African Charter) expressly forbids discrimination of any form by providing that 'every individual shall respect and consider other persons without discrimination, and to maintain relations aimed at promoting, safeguarding and reinforcing mutual respect and tolerance'.⁷²

Evidence of discrimination is when data subjects suffer adverse treatments not justified by their performance.⁷³ As a continent, Africa is made up of divergent ethnic groups, nationalities and heterogeneous people cohabiting across the continent. This means that distinct cultures, languages,⁷⁴ skin colour,⁷⁵ and so forth, form some of the characterisations

70 Algorithmic bias has been defined as the situation where machine learning programs inherit social patterns reflected in their training data without any directed effort by programmers to include such biases. See G Johnson, 'Algorithmic bias: on the implicit biases of social technology' (2020) 1-21 Synthese <https://philpapers.org/rec/JOHABO-5> (accessed 14/09/2021).

71 B Cowgill and others 'Biased programmers? Or biased data? A field experiment in operationalising AI ethics' in Proceedings of the 21st ACM Conference on Economics and Computation (1 June 2020) 2, 22-23, <https://ssrn.com/abstract=3615404> (accessed 16 September 2020).

72 Organisation of African Unity (OAU) African Charter on Human and Peoples' Rights (African Charter) 27 June 1981, CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982).

73 Cowgill and others (n 71) 3.

74 This might be relevant for voice recognition technology.

75 This might be relevant for facial recognition technology.

of Africans. For instance, it has been found in some cases that AI has failed to recognize or has erroneously recognised persons from minority races largely due to the use of non-representative training data and engineers at the machine-learning phase of the AI system.⁷⁶ Hypothetically, if non-representative data/engineers is used in an African context, AI systems developed by engineers of West African descent may not identify North Africans and *vice versa*. This is because said AI would have been trained with data that accommodates the physical features of certain tribes/ethnic groups to the detriment of others. Therefore, AI systems that will effectively and unbiasedly serve the African populace must employ data that is representative of the divergent ethnic groups, nations and people that make up the continent. Engineers must also be from divergent descent and/or must take the ethnic divergence of the continent into consideration when developing AI. In resolving this concern, it is necessary that representative training data that reflects all ethnic groups are used.⁷⁷ An equality impact assessment (EIA) aimed at identifying and remediating bias and inequity in AI systems before they are released for public use could also be helpful in mitigating identified biases.⁷⁸ To develop such an EIA, the input of stakeholders across the production lifecycle of the AI industry will be necessary to ensure that a truly representative and effective assessment is developed.

AI systems are able to make automated decisions that affect the fundamental rights and freedoms of data subjects thereby constituting a data protection law concern. AI algorithms can be trained to assess the personal data of data subjects and determine their eligibility in various scenarios, such as obtaining loans and mortgages.⁷⁹ AI is also being used to determine the rate of recidivism for convicted persons with such AI being the basis for deciding whether persons accused of certain crimes will be eligible for parole⁸⁰ or will be forced to serve out the full length of their

76 A Harmon 'As cameras track Detroit's residents, a debate ensues over racial bias' *The New York Times* 18 July 2019, <https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html> (accessed 14 September 2020). -recognition-

77 Cowgill and others (n 71) 2.

78 For further readings, see Biotechnology and Biological Sciences Research Council 'Equality impact assessment guidance and template', <https://bbsrc.ukri.org/documents/equality-impact-assessment-guidance-template-pdf/> (accessed 14 September 2020).

79 D Faggella 'Artificial intelligence applications for lending and loan management' *Emerj* (3 April 2020), <https://emerj.com/ai-sector-overviews/artificial-intelligence-applications-lending-loan-management/> (accessed 17 September 2020).

80 NL Hillman 'The use of artificial intelligence in gauging the risk of recidivism' *ABA* (1 January 2019), https://www.americanbar.org/groups/judicial/publications/judges_journal/2019/winter/the-use-artificial-intelligence-gauging-risk-recidivism/ (accessed 7 September 2020).

sentence,⁸¹ and so forth. If not properly managed, this can significantly affect the fundamental rights and freedoms of data subjects. In respect of automated decision making, the focus legislations contain the following provisions:

Article 14(5) of the AU Convention provides that ‘a person shall not be subject to a decision which produces legal effects concerning him/her or significantly affects him/her to a substantial degree, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her’. Article 35(2) of the ECOWAS Act provides that ‘no decision that has legal effect on an individual shall be based solely on processing by automatic means of personal data for the purpose of defining the profile of the subject or evaluating certain aspects of their personality’. Section 35(1) of DPAK provides that ‘every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject’. Section 35(3) of DPAK provides that data controllers or data processors must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to reconsider the decision, or take a new decision that is not based solely on automated processing. Based on the provision of section 35(4) of DPAK, once the data controller or data processor receives the data subject’s request in accordance with section 35(3) DPAK, they are to consider and/or comply with the request and inform data subjects of the steps taken to comply with the request.

It would appear that the focus legislations fall short of the requirements needed for attaining data protection compliance in automated decision making. These legislations forbid decisions made solely by automated means where such decisions affect the rights and freedoms of data subjects. From the provisions of these laws, it would appear that automated decisions will be lawful where they are not the sole basis for making a decision. This could be the case where an automated decision is made subject to the oversight or review of a human person. The DPAK is more elaborate and goes further than the other two focus legislations. Data controllers and data processors are mandated to notify data subjects about decisions based solely on automated processing and the data subjects can request a review of the decision or taking a new decision that is not based solely on

81 K Hao ‘AI is sending people to jail and getting it wrong’ MIT Technology Review (21 January 2019), <https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/> (accessed 7 September 2020). For further readings on the use of AI in law enforcement, see AG Ferguson *The rise of big data policing: Surveillance, race, and the future of law enforcement* (2017).

automated processing. However, it still falls short of effectively protecting the rights of data subjects. The non-completeness of these provisions might result in some confusion in its interpretation. Some other standard features in the regulation of automated decision making are the rights of data subjects to obtain human intervention and review of automated decisions, to obtain an explanation, express their points of view and to contest automated decisions.⁸² The focus legislations are either silent or contain sparse provisions on some of the standard provisions in the data protection regulation of automated decisions. The approach of data protection law is to generally ensure that the principles of data protection in non-automated personal data processing and decision making are also achievable in non-automated personal data processing and decision-making activities.⁸³ The right to an explanation of algorithmic decisions is also understood to be a necessary right of data subjects in automated decision making, which is linked to the requirement that personal data should be processed in a transparent manner.⁸⁴ Possible considerations to achieve explainability by design have been said to include 'relying on an algorithmic technique which meets the intelligibility requirements sufficient to provide data subjects with relevant explanation(s) or enhancing an accurate algorithm with explanation facilities so that it can generate an intelligible explanation for its results'. Human intervention and review of automated decisions before said decisions are adopted are also very necessary as they help reduce the violations of the right to dignity of the human person that automated decisions pose.⁸⁵ Human review can also reduce or prevent any bias or discrimination that might result from the use of non-representative training data or engineers.

82 These provisions are reflected in Recital 71 and art 22 GDPR.

83 The right to the explanation of automated decision making is seen as an extension of the accountability and transparency principle. S Wachter, B Mittelstadt & L Floridi 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (28 December 2016) 1, <https://ssrn.com/abstract=2903469> (accessed 15 September 2020).

84 Wachter and others (n 83) 1, 4, 6.

85 Automated decision making affects the right to dignity of the human person because human beings might tend to trust automated decisions reached against them, thereby preventing the independent assessment of said decisions even when incorrect. For further reasons, see LA Bygrave 'Article 22. Automated individual decision-making, including profiling' in C Kuner, LA Bygrave & C Docksey *The EU General Data Protection Regulation (GDPR): A commentary* (2020) 526-528.

5.5 Data minimisation

AI systems are very prone to collecting more personal data than necessary for any processing activity.⁸⁶ This is partly because of the use of a substantial number of sensors and cameras that capture multiple categories of personal data. This principle requires that only data that is adequate, relevant and limited to what is necessary for the processing activity should be processed.⁸⁷ This principle does not require the reduction of data collection to an absolute minimum, but rather seeks to reduce data collection to the lowest possible level in relation to the purpose of processing.⁸⁸ The principle is reflected in article 13(3) (b) of the AU Convention, article 25(2) of the ECOWAS Act, and section 25(d) of DPAK. A possible example of the violation of this principle can be seen in the use of AI-based drones or other AI systems using cameras. If not properly managed, these drones will capture peoples' faces, homes, vehicle plate numbers and other categories of personal data capable of identifying natural persons with the effect being unlawful processing of personal data. If the data minimisation principle is to be reflected in AI systems, it is necessary for privacy by design⁸⁹ to be introduced early at the development phase of relevant AI systems. This will ensure that best practices that can prevent the capturing of unnecessary personal data can be introduced into AI systems at its development stage. For instance, where AI must capture human faces, the use of silhouettes that make human faces unidentifiable can be used once said faces are captured.

5.6 Accountability

The accountability principle requires that data controllers should be able to comply with the principles of data protection law.⁹⁰ Compliance with this principle would typically mean that data controllers have to document the rationale, principles and justifications that underlie their decisions. The focus legislations are silent on the accountability principle, which is not

86 C Melendez 'Data is the lifeblood of AI, but how do you collect it?' Infoworld (8 August 2018), <https://www.infoworld.com/article/3296044/data-is-the-lifeblood-of-ai-but-how-do-you-collect-it.html> (accessed 15 September 2020).

87 See art 5(1)(c) GDPR.

88 P Voigt & A von dem Bussche *The EU General Data Protection Regulation (GDPR): A practical guide* (2017) 90-91.

89 TJ Shaw *DPO handbook: Data protection officers under the GDPR, IAPP* (2018) 130-135.

90 For further readings on the accountability principle, see L Urquhart & J Chen 'On the principle of accountability: Challenges for smart homes and cybersecurity' (17 June 2020); A Crabtree, R Mortier & H Haddadi 'Privacy by design for the internet of things: Building accountability and security' (13 July 2020), <https://ssrn.com/abstract=3629119> (accessed 15 September 2020).






















good for the overall data protection law compliance of AI systems.⁹¹ This principle will be particularly essential to the data protection compliance of AI systems because of the non-regulation of various matters of data protection law compliance. The requirement to be able to demonstrate compliance with relevant data protection laws will put data controllers in a position where they are bound to ensure that they remain compliant with minimum thresholds of data protection law compliance for the fear that these decisions can be holistically reviewed by regulators in future. The fear of being sanctioned and/or fined based on documented information can motivate data controllers to strive towards compliance.

At the rate at which AI is growing on the continent, it is necessary for African countries to invest in the education of Africans on the legal (including data protection law) consequences of AI systems. This will serve the dual function of educating data controllers about measures to take towards compliance with relevant laws while data subjects will also be better educated about their rights and will pursue its enforcement as a result. Privacy impact assessments (PIAs) and privacy by design are two critical measures that will help identify data protection risks and introduce data protection law principles into AI systems at the very inception of the processing activity respectively. In the absence of adequate data protection laws, ethics will become very important to data protection law regulation. An appeal to the adoption of ethics in the regulation of data protection (in AI systems) is tantamount to an appeal to the moral compass of data controllers/processors to comply with minimum principles of data protection law because it is the right thing to do.⁹² The problem with this approach is that data controllers/processors might not be very motivated to follow minimum standards for data protection compliance for reasons that include the lack of oversight. In such a scenario, one cannot help but wonder 'who will guard the guards?' The tendency might be for data controllers/processors to adopt the standards of compliance that favour them at any given time, thereby creating selective compliance with data protection principles. Despite its shortcomings, ethics could still be helpful in attaining some minimum level of compliance especially in regions with dormant law makers. Data protection ethics can be implemented into AI systems through sectoral regulatory bodies that will seek to protect the rights of data subjects by holding data controllers/processors accountable. For instance, respective medical associations can regulate data protection

91 Only DPAK contains selective applications of the accountability principle for specific processing activities. See secs 31(2)(d), 36, 49(2) & 52(2) of DPAK.

92 L Floridi & M Taddeo 'What is data ethics?' Oxford Internet Institute (2016) 5. See also K O'Keefe & D O'Brien *Ethical data and information management* (2018) 39-49.

concerns in AI systems being used in medical practice by setting guidelines for protecting personal data.

Identified concerns	AU convention	ECOWAS Act	DPAK
Legal basis			
Transparent data processing			
Purpose limitation			
Algorithmic bias			
Algorithmic decision making			
Data minimisation			
Accountability			

The table above summarises the level of compliance of AI with selected requirements of data protection law. The ‘red’ circles represent complete non-compliance under the focus legislations; the ‘yellow’ circles represent those requirements that are partially compliant under the focus legislations. ‘Green’ circles would have represented those requirements that are compliant under the focus legislations. Unfortunately, none of the requirements can be said to be fully compliant. This shows that the usage of AI in Africa is not compliant and warrants more work if compliance is to be achieved.

6 Some implications of inadequate data protection law regulations for artificial intelligence systems

The inadequacy or non-existence of adequate AI-related considerations in data protection regulatory instruments poses risks not only to the rights of data subjects but also to the acceptance of AI as a legitimate member of our mainstream society. Some of these attendant risks that could emanate

from the use of AI underlie the suspicions that surround AI generally.⁹³ For these suspicions to be neutralised and for AI to attain legitimacy and trust in society, attendant risks must be identified, reviewed and resolved in accordance with applicable laws and taking the rights of data subjects into consideration.

The lack of adequate data protection laws in African countries will make the continent a testing ground for data processing activities that otherwise are unlawful in the home countries of multinational data controllers, with residents of the African continent being the guinea pigs for such unlawful processing activities. The same argument will apply where the existing data protection laws are poorly enforced. In practice, it is not very difficult to find data processing activities where data controllers under the guise of providing a service unlawfully process personal data in African countries in a manner that is unlawful in their home countries.⁹⁴ While such data controllers undoubtedly act in an unethical manner,⁹⁵ it behoves Africa(ns) to change the narrative by taking the enactment and enforcement of very strict data protection laws very seriously. Another disturbing incidence of this occurrence is the violation of the right to the dignity of the human person occasioned by this violation of the right to data protection. As noted by the European data protection supervisor, 'privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of ameliorating the possible erosion of privacy and dignity through large scale personal data processing'.⁹⁶ Therefore, violations of the right to data protection are also tantamount to violations of the right to the dignity of the human person, particularly because of the close relationship between personal data and who we are and can become.⁹⁷ The possible risks that may arise from the unlawful processing operations carried out by AI are heightened by the fact that such processing operations are large scales possibly covering multiple countries. The importance of proper regulations to prevent Africa

93 'Report shows consumers don't trust artificial intelligence' *Fintech news* (4 December 2019), <https://www.fintechnews.org/report-shows-consumers-dont-trust-artificial-intelligence/#:~:text=A%20new%20report%20released%20by,person%20to%20help%20make%20decisions>. (accessed 15 September 2020).

94 See E Salami 'Nigerian data protection law: The effectiveness of the Nigerian Data Protection Bill as a tool for fostering data protection compliance in Nigeria' (2019) 43 *Datenschutz Datensich* 579, <https://ssrn.com/abstract=3614335> (accessed 21 September 2020).

95 R Densmore *Privacy program management* (2013) 19.

96 European Data Protection Supervisor 'Opinion 4/2015: Towards a new digital ethics data, dignity and technology' (2015).

97 L Floridi 'The ontological interpretation of informational privacy' (2005) 7 *Ethics and Information Technology* 185-200.

from being a testing ground for unlawful processing activities cannot be overemphasised and must be given utmost attention.

The lack of adequate data protection regulations in the use of AI can also inhibit trade between African countries and their counterparts in countries where data protection law is properly regulated. For instance, African companies using AI for targeted marketing⁹⁸ in European Union (EU) countries will have to comply with the GDPR since they are targeting persons within the EU.⁹⁹ In today's global economy, personal data processing is a fundamental aspect of trade and business, and Africa stands to benefit significantly from having a compliant level of data protection law. Where African companies are not compliant with data protection law, their foreign counterparts will be skeptical about engaging them in businesses, thereby limiting trade for African businesses. Furthermore, the lack of data protection law will hinder the growth of businesses such as data-based businesses (for instance, 'cloud storage as a service'). This is because should the continent be tagged as being a non-compliant data protection region, such data-based businesses will not grow, which will be unfortunate on a continent that is in dire need of economic development.

7 Conclusion

Based on the analysis carried out in this chapter, Africa (and African countries) must re-examine their data protection laws to ensure that data protection law complies with the realities of an AI. Based on the focus legislations, decent data protection laws are already in existence across the continent, and two major steps are needed if African countries are to consolidate on this in the use of AI. First, Africa and African countries must be willing to revisit some of the provisions in their data protection legislations to permit amendments that arise in light of AI. Second, supervisory and regulatory authorities must take the enforcement of data protection somewhat more seriously by publishing guidance documents, making regulations to plug new gaps identified in the law, investigating alleged violations of data subject rights, conducting random audits, etc. Through these measures, the continent can control the impact of AI within the context of AI and reduce the mistrust that it has gathered overtime, thereby giving AI more legitimacy as a useful addition to the human society. Failure to do this will result in the violation of the data

98 AI systems have been developed for use in targeted marketing. See 'How AI is used in targeted marketing' (17 September 2020), <https://azati.ai/artificial-intelligence-targeted-marketing/> (accessed 21 September 2020).

99 See art 3 GDPR.

protection rights of a vast number of Africans and will slow down the acceptance of AI into the mainstream of the African economic life.

References

- Adaramola, Z ‘Why Africa is backward in technology – NOTAP’ (21 June 2012, All Africa)
- Bello, I ‘Beginners’ guide to artificial intelligence “AI”’ (17 July 2017) Medium
- Bode, K ‘Researchers find “anonymized” data is even less anonymous than we thought’ (Motherboard)
- Boyd, D & Crawford, K ‘Six provocations for big data’ A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011
- Bygrave, L A Data Protection Law: Approaching Its Rationale, Logic and Limits Information Law Series, Volume 10, (2002) 58.
- Bygrave, LA ‘Article 22. Automated individual decision-making, including profiling’ in Kuner, C, Bygrave, LA & Docksey, C (eds) *The EU General Data Protection Regulation (GDPR): A commentary* (OUP 2020)
- Carey, P *Data protection: A practical guide to UK and EU law* (OUP 2018)
- Castelluccia, C & Le Métayer, D ‘Understanding algorithmic decision-making: Opportunities and challenges’ European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 624.261 – March 2019
- Cowgill, B and others ‘Biased programmers? Or biased data? A field experiment in operationalising AI ethics’ in Proceedings of the 21st ACM Conference on Economics and Computation (1 June 2020) 2
- Crabtree, A and others ‘Privacy by design for the internet of things: Building accountability and security’ (13 July 2020, SSRN)
- Enev, M and others ‘Automobile driver fingerprinting’ (2016) 1 *Proceedings on Privacy Enhancing Technologies*
- Faggella, D ‘Artificial intelligence applications for lending and loan management’ (3 April 2020, Emerj)
- Ferguson, AG *The rise of big data policing: Surveillance, race, and the future of law enforcement* (New York University Press 2017)
- Finlay, S *Artificial intelligence and machine learning for business: A no-nonsense guide to data driven technologies* (2018)
- Floridi, L & Taddeo, M ‘What is data ethics?’ Oxford Internet Institute (2016) 5
- Floridi, L ‘The ontological interpretation of informational privacy’ (2005) 7 *Ethics and Information Technology* 185

- Greenleaf, G & Bertil, C 'Comparing African data privacy laws: International, African and regional commitments' (2020) *University of New South Wales Law Research Series*
- Hao, K 'AI is sending people to jail and getting it wrong' (2019 *MIT Technology Review*)
- Harmon, A 'As cameras track Detroit's residents, a debate ensues over racial bias' *The New York Times* (18 July 2019) recognition-
- Harrington, C 'Improving access to sexual health education in Kenya with artificial intelligence' (15 January 2020, Humans of Machine Learning)
- Herrmann, A and others *Autonomous driving: How the driverless revolution will change the world* (Emerald Publishing 2018)
- Hillman, NL 'The use of artificial intelligence in gauging the risk of recidivism' (1 January 2019, ABA)
- Jackson, H 'Information provision obligations' in Ustaran, E (ed) *European data protection law and practice* (International Association of Privacy Professionals 2018)
- Kaplan, J *Artificial intelligence: What everyone needs to know* (OUP 2016)
- Koroma, DSM 'Traditional forms of communication of the Malimba of Sierra Leone' (2018) 10.
- Lachlan, U & Jiahong, C 'On the principle of accountability: Challenges for smart homes and cybersecurity' (17 June 2020)
- Malik, N & Singh, PV 'Deep learning in computer vision: Methods, interpretation, causation and fairness' (28 May 2019)
- Malinga, S 'SA not ready for autonomous vehicles' (7 October 2020, ITWeb)
- McCarthy, J 'What is artificial intelligence?' (12 November 2007), <http://jmc.stanford.edu/articles/whatisai.html> (accessed 10 September 2020)
- Melendez, C 'Data is the lifeblood of AI, but how do you collect it?' (8 August 2018, Infoworld)
- Miriri, D 'Rwandan medical workers deploy robots to minimise coronavirus risk' (5 June 2020, World Economic Forum)
- O'Keefe, K & O'Brien, D *Ethical data and information management* (Kogan Page 2018)
- Odotola, A 'FG acquires profiling robots for airport' (27 June 2020, Nairametrics)
- Pierce, R 'Machine learning for diagnosis and treatment: Gymnastics for the GDPR' (2018) 4 *EDPL* 339

- Rosen, JW 'Zipline's ambitious medical drone delivery in Africa' (8 June 2017, MIT Tech Review)
- Russell, SJ & Norvig, P *Artificial intelligence: A modern approach* (Prentice Hall 2010)
- Salami, E 'Autonomous transport vehicles versus the principles of data protection law: Is compatibility really an impossibility?' (2020) *International Data Privacy Law Journal*
- Salami, E 'Nigerian data protection law: The effectiveness of the Nigerian Data Protection Bill as a tool for fostering data protection compliance in Nigeria' (2019) 43 *Datenschutz Datensich* 579
- Shacklett, M 'Repurpose big data to get more analytics bang for your bucks' (28 January 2014, Tech Republic)
- Shaw, TJ *DPO handbook: Data protection officers under the GDPR* (IAPP 2018)
- Sorkin, DE 'Technical and legal approaches to unsolicited electronic mail' (2001) 35 *USF Law Review* 325
- Stone, P and others 'Artificial intelligence and life In 2030: Report of the 2015-2016 Study Panel' (September 2016, Stanford.edu)
- Sweeney, L 'Matching known patients to health records in Washington State data' (5 June 2013)
- Tay, J and others 'Application of computer vision in the construction industry' (19 November 2019)
- Turing, AM 'Computing machinery and intelligence' (1950) 59 *Mind* 433
- Van der Velde, N 'Speech recognition technology overview' (8 July 2019, Globalme Language and Technology)
- Voigt, P & Von dem Bussche, A *The EU General Data Protection Regulation (GDPR): A practical guide* (Springer 2017)
- Wachter, S and others 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (28 December 2016) 1

5

AFRICAN DATA PROTECTION LAWS AND ARTIFICIAL INTELLIGENCE – REGULATION, POLICY AND WAYS FORWARD*

Moritz Hennemann

Abstract

The chapter engages with the approaches to AI by the data protection laws in Africa, including at the level of regional economic communities (RECs) and the African Union (AU) level. It shall be evaluated if and to what extent respective approaches specifically regulate AI, and to what end. It is targeted at the question of whether specific patterns can be identified that might serve as an approximation to a unique African approach to AI and data protection. On this basis, the potential for specific (future) instruments will be considered.

1 Introduction

Artificial Intelligence (AI) is a regulatory challenge to societies worldwide. Regulators must decide on an adequate (legal) framework for the ‘development’ and usage of AI. This decision comes along with fundamental questions. The innovation potential and the associated risks for individuals, societies, and states have to be balanced out. Answers must also be provided to the question regarding to what extent one shall facilitate or restrict the usage of AI. This process can also be framed as a ‘competition’ between different regulatory instruments¹ – and there is obviously no ‘right’ solution, as different legal traditions, cultural settings, and societal values will necessitate different approaches.

* This chapter is based on a conference paper presented at the Centre for Human Rights, University of Pretoria’s conference ‘Privacy and data protection law and practice in Africa – Challenges and prospects’. I do thank my former academic research assistants, Dr Patricia Boshe and Ricarda von Meding, for their helpful preparatory research, their handling of the various (legislative) documents, and their critical thoughts and feedback along the way. This work was supported by the Bavarian State Ministry of Science and Culture. The manuscript was finalised in January 2021; later developments could not be considered.

1 For details with respect to data protection law see M Hennemann ‘Wettbewerb der Datenschutzrechtordnungen’ (2020) 84 *Rabel Journal of Comparative and International Private Law* 864.

The term ‘Artificial Intelligence’ has been used in various contexts. In this chapter, AI refers to deploying algorithms that are not hierarchical programmed (pre-structured when-if-scenarios), but adaptable. Their (changing) parameters are not (even theoretically) fully foreseeable in advance – thereby, also their output (and the contexts in which those outputs might be of use) are not known and cannot be predicted beforehand. This process is also framed as ‘self-learning.’ Respective algorithms (constantly) derive patterns through processing non-personal and / or personal data. This is also to say that the identified patterns are ‘path-dependent’ on the used set of data – including the possibility that biases in the data spill over to the patterns identified. These algorithms are used in many scenarios and are labelled as ‘weak’ AI (non-existing ‘strong’ AI prerequisites some sort of ‘consciousness’ of the algorithm).

The technological realities of AI lead to numerous questions in different fields of law.² First and foremost, data laws are specifically relevant in this context. They form a significant regulatory instrument for AI as non-personal and/or personal data is the ‘resource’ for AI. While the processing of non-personal data is largely unregulated / left to contractual agreements, the processing of personal data triggers the domain of data protection law – which shall be the focus of this chapter. Data protection law is a legal field directed towards counterbalancing (potential) threats to personal data/privacy. However, it must be made clear from the outset that AI-based applications do not necessarily go along with a general threat to personal data/privacy. AI can also benefit privacy and data protection if respective applications are used exactly for privacy purposes (such as Personal Information Management Systems).

Nevertheless, at least traditional data protection regulation approaches do generally restrict the processing of personal data in the context of AI. Thereby, data protection regulation poses some basic challenges to AI – or to phrase it differently: there is specific tension between AI and data protection laws, for example, with regard to the data protection law principles of data minimisation and purpose limitation. These principles are, from the outset, at odds with the characteristics mentioned above of AI, especially the need for adequate data sets and unforeseeable outcomes. On this basis, for example, the European Union (EU) data protection law, the General Data Protection Regulation (GDPR), is strongly criticised in

2 The Law Library of Congress ‘Regulation of artificial intelligence in selected jurisdictions’ (January 2019) gives an overview to general AI regulation in selected jurisdictions worldwide. For selected African jurisdictions see 119 ff (in parts), 129 ff; see also the comparative summary (including maps) by J Gesley at 1 ff. See eg with respect to competition law M Hennemann ‘Artificial Intelligence and competition law’ in T Wischmeyer & T Rademacher (eds) *Regulating Artificial Intelligence* (2020) 361.

significant parts of the literature.³ The result is an ongoing debate about whether and to what extent specific (less strict or stricter) data protection rules with respect to AI should be implemented.

Against this background, this chapter will analyse the approach to AI by the current data protection laws in Africa, including at the level of Regional Economic Communities (RECs) and the African Union (AU) level.⁴ It will first evaluate the extent to which respective approaches *specifically* regulate AI. On this basis, second, this chapter gives an overview of options for specific future instruments. This chapter does not engage the general application of African data protection laws to AI.⁵

2 African data protection laws and artificial intelligence: The current state

As a first step, this chapter gives an overview of the approaches to AI by the current (2020) African data protection laws, including at REC and the AU levels.

2.1 General overview

There seems to be no *AI-specific* data protection regulation in African states, at the AU⁶ level or at the level of the RECs (as of 2020). The AU Digital Transformation Strategy for Africa, adopted in February 2020, acknowledges the lack of AI-specific regulation in Africa.⁷ The ‘Resolution on the need to undertake a Study on human and peoples’ rights and artificial intelligence (AI), robotics and other new and emerging technologies in

3 For details see Y Lev-Aretz & KJ Strandburg ‘Privacy Regulation and Innovation Policy’ (2020) 22 *Yale Journal of Law & Technology* 256; T Zarsky ‘Incompatible: The GDPR in the Age of Big Data’ (2017) 47 *Seton Hall Law Review* 995.

4 For a detailed introduction to the current state see G Greenleaf & B Cottier ‘Comparing African data privacy laws: International, African and regional commitments’ (2020) 32 *University of New South Wales Research Series* and P Boshe and others ‘African data protection laws: Current regulatory approaches, policy initiatives, and the Way Forward’ (2022) 3 *Global Privacy Law Review* 56.

5 See in this regard the respective conference contributions / chapters in this book.

6 See also Internet Society and Commission of the African Union ‘Personal Data Protection Guidelines for Africa’ (May 2018) https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 01 October 2020), highlighting at 25 the need of policymakers to engage with: ‘implications of emerging technologies (data mining, machine learning and Artificial Intelligence; autonomous systems; Internet of Things, etc.)’.

7 African Union ‘The Digital Transformation Strategy for Africa’ (2020-2030) <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> (accessed 1 October 2020); see 43: ‘Currently in Africa, emerging technologies are unregulated.’

Africa' (February 2021) of the African Union Commission points to the fact 'that while AI companies, as well as organisations and businesses that use AI technologies ... have a significant impact on human rights protection in Africa, there is no comprehensive framework governing their operations to ensure that they comply with human rights obligations on the continent.'⁸ It underlines 'the need for a comprehensive governance framework on AI technologies ... in Africa in a way that enhances human rights protection on the African continent including protection of the ownership of data on individuals experience in the digital sphere'⁹.

However, reviewing the situation through the lens of data protection laws in African states, the following point must be made from the outset: This is *not* to say that laws do not regulate AI in any manner. Data protection laws in Africa do exist and regulate the processing of personal data which also covers respective AI-based processes. The data processor is in this context *inter alia* bound by data protection principles, rules and limits set out by respective laws, especially data subject's rights. However, the identified legislation may be classified as general and *not AI-specific* data protection regulation. This does not mean African countries do not consider or test additional or complementary legislation and administrative structures.

2.2 Selected jurisdictions

The following section highlights the respective approaches taken in regards to data protection in the selected jurisdictions.¹⁰ The section will refer to AI Strategies and legislation, but will not discuss constitutional rights to privacy in the respective countries.

8 ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, <https://www.achpr.org/sessions/resolutions?id=504>.

9 As above.

10 The following criteria led to the selection of specific jurisdictions: First, the following five jurisdictions were classified as the top five African jurisdictions in respect of 'Government AI Readiness' by the Oxford Insights and the International Development Research Centre in 2019 (Oxford Insights and the International Development Research Centre 'Government AI Readiness Index 2019' (2019) <https://www.oxfordinsights.com/ai-readiness2019> (accessed 01 October 2020): Kenya (no 1 in Africa; no 52 globally), Tunisia (no 2 / no 54), Mauritius (no 3 / no 60), South Africa (no 4 / no 68), and Ghana (no 5 / no 75)). Second, the representation of RECs in different data protection frameworks in Africa (e. g. EAC, SADC, ECOWAS) was considered. Third, the enforcement especially by Mauritius of data protection laws and the awareness shown for data protection laws by, for example, the Ghanaian Data Protection Commission which organises by conferences and awareness programmes were considered.

2.2.1 *AI strategies*

There are various initiatives concerning AI at the strategic level in African states. Kenya, for example, has engaged with the usage of AI in different ways. In July 2019, the Kenya Ministry of Information, Communications and Technology published the report of the Distributed Ledgers Technology and Artificial Intelligence Taskforce ‘Emerging Digital Technologies for Kenya – Exploration & Analysis’ (Taskforce Report).¹¹ In April 2019, Kenya conducted the AI for Development Workshop as part of the AI Network of Excellence in Sub-Saharan Africa.¹² The Taskforce Report highlights the disruptive nature of AI, the potentials for the public and the private sector, and underlines the need to develop ‘effective regulations to balance citizen protection and private sector innovation’.¹³ The Taskforce Report explicitly refers to ‘concerns about data privacy’ as discussion points.¹⁴ The Taskforce correctly highlights that ‘AI may encourage the proliferation of surveillance states and digital totalitarianism. To fully optimise the benefits from AI, government data will be centralised, and such centralisation carries the risk that government could abuse its power and infringe on the privacy of its citizens.’¹⁵

Mauritius has handed down the AI Strategy of 2018¹⁶ and the Digital Mauritius 2030 Strategic Plan¹⁷. The Strategy highlights (1) the usage of regulatory sandboxes for AI in order to *inter alia*, evaluate the adjustment to current legislation as well as the possibility of establishing an AI Council to monitor deployments and to develop new legislation, (2) a standing AI Committee on Ethics, and (3) governmental data centres.¹⁸ The Strategic Plan also envisages the creation of the AI council and ‘re-engineering of user processes before [the] application of technology’ and creation of an

11 Kenya Ministry of Information, Communications and Technology (Distributed Ledgers Technology and Artificial Intelligence Taskforce) ‘Emerging Digital Technologies for Kenya – Exploration & Analysis’ (July 2019).

12 Notes and videos of the workshop are available at: <https://www.idrc.ca/en/news/workshop-launch-ai-network-excellence-sub-saharan-africa> (accessed 01 October 2020).

13 Kenya Ministry of Information, Communications and Technology (n 11) 9, 10, 39 et seq.

14 Kenya Ministry of Information, Communications and Technology (n 11) 42.

15 Kenya Ministry of Information, Communications and Technology (n 11) 43.

16 Mauritius Artificial Intelligence Strategy: A Report of the Working Group on Artificial Intelligence (November 2018).

17 Ministry of Technology, Communication and Innovation, Digital Mauritius 2030 Strategic Plan (2018).

18 Mauritius Artificial Intelligence Strategy (n 16) at 3 et seq.

‘enabling environment’ for the management of big data.¹⁹ The Strategic Plan additionally points to the fact that ‘[t]he Mauritian data protection and privacy law seeks as much as possible to balance [the] different concerns and interests, ideally in a way that does not unnecessarily hamper the scope for technological development.’²⁰

South Africa has established a Presidential Commission on the Fourth Industrial Revolution (4IR)²¹ that published an extensive report.²² The report highlights regarding AI that an “ethical and transparent use of these new technologies” is of vital importance.²³ Pointing to data protection, the report proposes *inter alia* in-land data centres²⁴, a national open data strategy²⁵, a future ‘[f]ocus on data privacy and data protection laws and regulations’²⁶, and protection through ‘South Africa’s Information Regulator’ to help ‘South Africa meet international privacy standards’²⁷. The report states that ‘data management’ should be placed ‘at the cross-cutting base of the state and public-private partnerships’.²⁸

2.2.2 Legislation

At the regulatory level, Kenya recently enacted the Data Protection Act of 2019²⁹ and the Computer Misuse and Cybercrimes Act of 2018.³⁰ The Kenya Data Protection Act does not *specifically* regulate AI, only the general rules of data processing (including automated decisions) apply (compare Sec. 4, 25, 30 and 35). The same is true for Mauritius (Data Protection Act of 2017),³¹ South Africa (Protection of Personal

19 Digital Mauritius 2030 Strategic Plan (n 17) 2, 6, 24, 32, 34 et seq.

20 Digital Mauritius 2030 Strategic Plan (n 17) 36.

21 Department of Telecommunication and Postal Services ‘Notice 209 of 2019’ *RSA Government Gazette* 42388.

22 Dept. of Communications and Digital Technologies ‘Report of the Presidential Commission on the 4th Industrial Revolution’ *RSA Government Gazette* 43834 (October 2020).

23 Department of Communications and Digital Technologies (n 22) 149.

24 Department of Communications and Digital Technologies (n 22) 300.

25 Department of Communications and Digital Technologies (n 22) 302.

26 Department of Communications and Digital Technologies (n 22) 322.

27 Department of Communications and Digital Technologies (n 22) 325.

28 Department of Communications and Digital Technologies (n 22) 138.

29 Act 24 of 2019. See also AB Makulilo & P Boshe ‘Data protection in Kenya’ in Makulilo (ed) *African Data Privacy Laws* (2016) 317.

30 Act 5 of 2018.

31 Act 20 of 2017. See for details AB Makulilo ‘The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius’ (2021) 25 *The International Journal of Human Rights* 117; AB Makulilo ‘Data protection of the Indian

Information Act of 2013,³² Ghana (Data Protection Act of 2012),³³ and Tunisia (Data Protection Law in 2004).³⁴

2.3 Summary

None of the aforementioned rules *specifically* regulate AI yet – despite different AI strategies pointing to that end. AI is (only) covered by the respective general rules on data processing in the respective states.

3 A comparative look at the European Union and the GDPR

The aforementioned national sets of norms generally follow the lines of the Data Protection Directive 1995 (DPD) and the GDPR. The European Union itself has no *AI-specific* data protection regulation. Although the GDPR was aimed at ‘aligning’ EU data protection law to modern technologies, article 22 GDPR, for example, only generally regulates ‘automated individual decision-making.’ This rule is complemented by article 13(2)(f) GDPR (identical article 14(2)(g) GDPR). The latter norm stipulates that ‘the controller shall ... provide the data subject with the following further information ... the existence of automated decision-making, including profiling, ... at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.’ Article 15(1)(h) of GDPR stipulates an additional right to obtain a confirmation on the existence of a respective automated decision-making. As it is true for the aforementioned pieces of regulation, the general GDPR rules for data processing apply.³⁵

On the policy level, the European Commission published its communication on ‘a European strategy for data’ in February 2020.³⁶ The communication highlights the integral part the existing data

Ocean Islands: Mauritius, Seychelles, Madagascar’ in Makulilo (n 29) at 277.

32 Act 4 of 2013. See also A Roos ‘Data Protection Law in South Africa’ in Makulilo (n 29) at 189.

33 Act 843 of 2012. See also DN Dagbanja ‘The Right to Privacy and Data Protection in Ghana’ in Makulilo (n 29) 229.

34 Loi portant sur la protection des données à caractère personnel n° 2004-63 du 27 juillet 2004. See also AB Makulilo ‘Data protection in North Africa: Tunisia and Morocco’ in Makulilo (n 29) 27.

35 See in this regard European Commission ‘White Paper – On Artificial Intelligence – A European approach to excellence and trust’ COM(2020) 65 final at 10.

36 European Commission ‘Communication – A European strategy for data’ COM(2020) 66 final.

protection law plays for any future European regulation. However, it is possible that the EU might take steps to '[ensure] legal clarity in AI-based applications.'³⁷ The White Paper on AI states: '[S]ome specific features of AI (e.g., opacity) can make the application and enforcement of [the EU] legislation more difficult. For this reason, there is a need to examine whether current legislation can address the risks of AI and can be effectively enforced, whether amendments of the legislation are needed, or whether new legislation is needed. Given how fast AI is evolving, the regulatory framework must provide room for further developments. Any changes should be limited to clearly identified problems for which feasible solutions exist.'³⁸ The White Paper underlines the AI-related threats to data protection: 'By analysing large amounts of data and identifying links among them, AI may also be used to retrace and de-anonymise data about persons, creating new personal data protection risks even in respect to datasets that per se do not include personal data.'³⁹

So, modifications of EU data protection law to regulate AI *specifically* are likely. For example, the European Commission underlines the need for transparency with respect to capabilities, limitations, and purposes. In addition, the Commission states: '[C]itizens should be clearly informed when they are interacting with an AI system and not a human being. ... [A]dditional requirements may be called for to achieve the abovementioned objectives. If so, unnecessary burdens should be avoided. Therefore, no such information needs to be provided, for instance, in situations where it is immediately obvious to citizens that they are interacting with AI systems.'⁴⁰

4 **Balancing innovation and potential risks: The way forward**

The Kenya Taskforce rightly concluded: 'Ultimately, the challenge for regulation is how to balance supporting innovation and competition while protecting customers, market integrity, financial stability and human life.'⁴¹ To state the obvious, any AI-related regulation has to

37 European Commission 'Artificial Intelligence' <https://ec.europa.eu/digital-single-market/en/artificial-intelligence> (accessed 01 October 2020).

38 European Commission (n 35) 10.

39 European Commission (n 35) 11. See also fn 34 herein: 'The [GDPR] and the ePrivacy Directive (new ePrivacy Regulation under negotiation) address these risks but there might be a need to examine whether AI systems pose additional risks. The Commission will be monitoring and assessing the application of the GDPR on a continuous basis.'

40 European Commission (n 35) 20.

41 Kenya Ministry of Information, Communications and Technology (n 11) 42.

strike a balance between threats and opportunities. Innovation should be possible, potential risks should be mitigated sensibly. On this basis, the potential for specific future instruments, may it be hard or soft law and at different levels, are considered. Furthermore, and specifically with respect to Africa, the African Union Commission correctly “[emphasises] the need for sufficient consideration of African norms, ethics, values, such as ubuntu, communitarian ethos, freedom from domination of one people by another, freedom from racial and other forms of discrimination in framing of global AI governance frameworks”⁴².

4.1 General remarks on AI regulation

For any future regulation of AI, the regulatory model to be applied, whether on the national, the REC or the level of the African Union, has to be discussed.⁴³ Legislators will have to decide whether to change from the current ‘one-size-fits-all’-regulatory regime and to take the ostensibly more burdensome path of a sector-specific risk assessment which would then inform the approach to be taken. Regulatory sandboxes could also be used to test and evaluate specific types of regulation.⁴⁴ This comes along with a framework of accountability and parameters for an affirmation process for AI applications.⁴⁵ Obviously, further conditions to optimise the efficacy and to mitigate risks should be considered. A special focus on the quality of datasets as well as their regional relevance seems to be beneficial.⁴⁶ Technical methods coming close to anonymisation of data should be considered thoroughly.⁴⁷ Furthermore, an essential ingredient is that consumers have a general understanding of the data processing being undertaken and its general purpose.⁴⁸ This requires a consideration of how such an understanding can be achieved and is dependent on the extent to which duties to inform are an adequate tool to achieve this.

42 ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, <https://www.achpr.org/sessions/resolutions?id=504>.

43 As above.

44 Kenya Ministry of Information, Communications and Technology (n 11) at 11, 14; Report of the Presidential Commission on the 4th Industrial Revolution (n 22) at 324.

45 R Calo ‘Artificial intelligence policy: A primer and roadmap’ 51 *U.C. Davis Law Review* 300 (2017); M Romanoff ‘Building ethical AI approaches in the African context’ *UN Global Pulse* 28 August 2019 <https://www.unglobalpulse.org/2019/08/ethical-ai-approaches-in-the-african-context/> (accessed 01 October 2020).

46 World Wide Web Foundation ‘Artificial Intelligence – Starting the policy dialogue in Africa’ (December 2017) at 7.

47 C Dwork ‘Differential Privacy’ (2007), <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf>; Calo (n 45).

48 Romanoff (n 45).

Personal information management systems (see below) could be a viable alternative.

4.2 What kind of privacy?

Any regulation is dependent on the determination of the kind of privacy it seeks to protect.⁴⁹ It therefore can be asked whether regulators focus on individual privacy (or individual data protection) or on ‘group privacy’.⁵⁰ Group privacy could either complement or substitute individual rights. Group privacy might be considered as a reflection of a community-orientated approach in data protection legislation, might be aligned to African norms, and especially to the socio-cultural principle of communalism popularly described as ubuntu⁵¹ – as highlighted by the African Union Commission before and by Art. 8(2) of the Malabo Convention (‘that any form of data processing ... [recognises] the rights of local communities’).

The future framework for individual data protection rights is linked to and dependent on the potential level of group privacy. On this basis, one might grant individual rights only on the basis of an AI sector-specific risk-based approach or in situations where processing of sensitive data takes place. In this regard, there should be an evaluation of the legal principles of traditional data protection laws principles, such as data minimisation and purpose limitation, as well as data subject’s rights. For example, one could consider the shortcomings of the right to explanation (equivalent to Art. 13, 14, 15 GDPR), especially the usefulness of the respective explanation. Parameters of even simple algorithms tend to be too complex to explain in relation to everyday scenarios. Furthermore, with respect to the right not be subject to automated or autonomous decision-making (equivalent to Art. 22 GDPR), it should be borne in mind that a ‘one-size-fits-all’ approach is likely to lead to an ‘overblocking’ of standard everyday

49 See P Boshe in chapter one of this book.

50 L Taylor and others (eds) *Group privacy: New challenges of data technologies* (2017); U Reviglio & R Alunge “‘I am datafied because we are datafied’: An ubuntu perspective on (relational) privacy’ (2020) 33 *Philosophy & Technology* 595; M Christen & M Loi ‘Two concepts of group privacy’ (2020) 33 *Philosophy & Technology* 207; Romanoff (n 45).

51 This refers to *Umuntu ngumuntu ngabantu abanye*, which can be translated as ‘a person is a person through other persons’. There is a link between the concept of *ubuntu* and African philosophy emphasizing collectivist human relationships, see P Boshe ‘Data Protection Legal Reforms in Africa’ (2017) University of Passau PhD Thesis 64 fn 386 with further references as well as PD Rwelamila and others ‘Tracing the African Project Failure Syndrome’ (1999) 6 *Engineering, Construction and Architectural Management* 335 and AB Makulilo “‘A Person is a Person through other Persons’ A critical analysis of privacy and culture in Africa’ (2016) 7 *Beijing Law Review* 192.

decisions and thus a sector-specific regulation or a regulation focused solely on the processing of sensitive data could be examined.

4.3 Societal data access

Any approach could go along with societal access to datasets. As long as respective data cannot be anonymised, the datasets might be used in defined circumstances to train AI applications, most likely on the basis of an open government approach.⁵² The use of open government data for societal good could be fostered. The Digital Transformation Strategy also suggests this approach. The Strategy favours open data and the interoperability of data and data systems.⁵³ It proposes adopting open data standards and policies⁵⁴ and defining technology standards⁵⁵. This is not to imply that the dataset has to be managed by the respective state. Governments could use a trusted intermediary which is supervised by various stakeholders, members of the civil society or regional or local communities – and accountable to them. In this respect, the Digital Transformation Strategy proposes ‘a high-level Enterprise Information Service Architecture (EISA) ... to promote and support inter-operability, open systems, ... and best practices’⁵⁶.

4.4 Data security and technical standard-setting

Data protection is not complete without regulation on data security. Technical standards need to be set, particularly with respect to AI applications. Such standard setting should be based on a risk assessment to prevent the misuse of personal data, thereby fostering trust in the particular application. Therefore, standards for AI design processes should be developed that support general transparency and accountability, whether in the private or public sector.⁵⁷ Database-related standards should, alongside other factors, aim to minimise discriminatory biases.⁵⁸ Security-related, AI might even help to guarantee and to check the strength and standard

52 World Wide Web Foundation (n 46) 7. See also Romanoff (n 45).

53 The Digital Transformation Strategy (n 7) 3, 34

54 The Digital Transformation Strategy (n 7) 3 & 22.

55 The Digital Transformation Strategy (n 7) 30 & 33

56 The Digital Transformation Strategy (n 7) at 29.

57 Romanoff (n 45).

58 Calo (n 45); Kenya Ministry of Information, Communications and Technology (n 11) 38, 43.

of data security.⁵⁹ In sectors with risky or sensitive data processing, the establishment of a certification structure should be considered. It has to be borne in mind that AI's 'self-learning' algorithms change and adapt. Any certification can only be a 'basic' test of the general structure, and not with respect to every 'outcome' of the algorithm. A certification structure could therefore entrust the certifying entities with monitoring duties.

The standard-setting and certification process does not need to be, and quite often cannot be, the exclusive remit of the state. Rather, entities or bodies might make use of external technical, legal, and political experts, either as committee members or as part of a public-private-partnership⁶⁰. The participation and integration of further stakeholders (for example, civil society, open source-community) might be an additional trust-building option. In this direction, the Digital Transformation Strategy proposes the establishment of a 'framework on data policy and management for Africa'⁶¹ and 'mechanism for regional cooperation and mutual assistance'.⁶²

4.5 AI privacy-enhancing applications

Taking a step back, one might finally conclude that in tech-driven times, privacy relating to technical applications might only be reached by the very use of tech by the individual. Starting from Antitrust Law, the concept of an 'algorithmic consumer' (*Gal/Elkin-Koren*)⁶³ has made its way through other fields of law. The underlying premise is that individuals use technical applications, acting in their own interest. AI is not only used in relation to the individual but *by* the individual.⁶⁴ Respective applications are normally labelled as bots or autonomous agents. From a data protection law perspective, this refers to Personal Information Management Systems (PIMS).⁶⁵ These systems – at odds with traditional data protection laws – administer the personal data of the individual, act on the basis of the individual's general preferences of the individual, and value different offers on the market respectively. Individuals could thus have access to a

59 E Segal 'The role of AI in data security' (19. July 2019) <https://datafloq.com/read/role-of-ai-data-security/6616> (accessed 01 October 2020).

60 Kenya Ministry of Information, Communications and Technology (n 11) at 11; Report of the Presidential Commission on the 4th Industrial Revolution (n 22) 138.

61 The Digital Transformation Strategy (n 7) 47.

62 As above.

63 MS Gal & N Elkin-Koren 'Algorithmic consumers' (2017) 30 *Harvard Journal of Law & Technology* 309.

64 Calo (n 45).

65 https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en (accessed 01 October 2020).

broader variety of services, overcome potential lock-in-effects, and foster competition for privacy and privacy-protecting services.

4.6 AI model laws for Africa?

Next to hard law approaches, which might not be easy to agree on, a medium term-goal could also be soft law instruments fostering AI regulation ('AI model laws'); for example, drafted by the African Union or the African RECs.⁶⁶ Such model might also be based – if that is found to be a sensible solution – on an new approach giving ubuntu, communities, and group privacy a more appropriate place in legislation.⁶⁷ Such an approach might neatly fit into the broader policy framework. The Digital Transformation Strategy rightly points to the fact that especially for an envisioned African digital single market, '[b]eing prepared for digital transformation and emerging technologies such as Artificial Intelligence (AI) ... is fundamental. Public policy, [l]egal and regulatory frameworks need to be up-to-date, flexible, incentive-based and market-driven to support digital transformation across sectors and across the continent regions.'⁶⁸ Policies should be 'designed based on a human-centred and holistic approach that also takes into account the local context and cross-cutting issues relevant to all stages of policy design and implementation.'⁶⁹

5 Conclusion

There is yet no *AI-specific* data protection rules exist in African states as in the EU and on the REC and AU levels (as of 2020). AI is only regulated 'along the way' in data protection law, by the general rules applicable to data processing. On the basis of the aforementioned arguments, this current state is evaluated – especially where beneficial effects with respect to privacy and data protection are possible, for example, using personal information management systems. The adjustment of regulatory instruments should be considered. Ideally, legal traditions, different cultural settings, and diverse societal values will frame future African instruments (and beyond). To this end, this chapter proposes that lawmakers consider: (1) the non-use of mere 'copies' of the GDPR or the DPD⁷⁰; (2) the integration of elements

66 'Toward a Network of Excellence in Artificial Intelligence for Development (AI4D) in sub-Saharan Africa' 3-5 April 2019. Such a model law would probably tackle not only questions of data protection law, but also other relevant fields of law.

67 ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, <https://www.achpr.org/sessions/resolutions?id=504>.

68 The Digital Transformation Strategy (n 7) at 7.

69 The Digital Transformation Strategy (n 7) 8.

70 See generally Hennemann (n 1).

of ‘group privacy’; (3) a risk-based approach for AI data protection law regulation; (4) enhancing the usage of AI, especially personal information management systems, by individuals; and (5) AI model laws at the REC or African Union level.

References

- Boshe, P 'Data protection legal reforms in Africa' PhD thesis, University of Passau, 2017
- Boshe, P and others 'African data protection laws: Current regulatory approaches, policy initiatives, and the way forward' (2022) 3 *Global Privacy Law Review* 56
- Calo, R 'Artificial intelligence policy: A primer and roadmap' (2017) 51 *UC Davis Law Review* 399
- Christen, M & Loi, M 'Two concepts of group privacy' (2019) 33 *Philosophy and Technology* 207
- Dagbanja, DN 'The right to privacy and data protection in Ghana' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)
- Dwork, C 'Differential privacy' (2007), <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf>
- Gal, MS & Elkin-Koren, N 'Algorithmic consumers' (2017) 30 *Harvard Journal of Law and Technology* 309
- Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments' (2020) 32 *University of New South Wales Research Series*
- Hennemann, M 'Wettbewerb der Datenschutzrechtordnungen' (2020) 84 *Rabel Journal of Comparative and International Private Law* 864
- Hennemann, M 'Artificial intelligence and competition law' in Wischmeyer, T and Rademacher, T (eds) *Regulating Artificial Intelligence* (Springer 2020)
- Internet Society & Commission of the African Union 'Personal Data Protection Guidelines for Africa' (May 2018) https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 1 October 2020)
- Lev-Aretz, Y & Strandburg, KJ 'Privacy Regulation and Innovation Policy' (2020) 22 *Yale Journal of Law & Technology* 256
- Makulilo, AB 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25 *The International Journal of Human Rights* 117
- Makulilo, AB "'A Person is a person through other persons" – A critical analysis of privacy and culture in Africa' (2016) 7 *Beijing Law Review* 192
- Makulilo, AB 'Data protection in North Africa: Tunisia and Morocco' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)

- Makulilo, AB 'Data protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagascar' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)
- Makulilo, AB & Boshe, P 'Data protection in Kenya' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)
- Rwelamila, PD and others 'Tracing the African project failure syndrome' (1999) 6 *Engineering, Construction and Architectural Management* 335
- Reviglio, U & Alunge, R "'I am datafied because we are datafied'": An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy & Technology* 595
- Romanoff, M 'Building ethical AI approaches in the African context' *UN Global Pulse* 28 August 2019 <https://www.unglobalpulse.org/2019/08/ethical-ai-approaches-in-the-african-context/> (accessed 01 October 2020)
- Roos, A 'Data protection law in South Africa' in Makulilo, AB (ed) *African Data Privacy Laws* (Springer 2016)
- Segal, E 'The role of AI in data security' (July 2019) <https://datafloq.com/read/role-of-ai-data-security/6616> (accessed 1 October 2020)
- Taylor, L and others (eds) *Group privacy: New challenges of data technologies* (Springer 2017)
- Zarsky, T 'Incompatible: The GDPR in the age of big data' (2017) 47 *Seton Hall Law Review* 995

PART III: Data privacy and vulnerable groups

6

DIGITAL VULNERABILITIES AND THE PRIVACY CONUNDRUM FOR CHILDREN IN THE DIGITAL AGE: LESSONS FOR AFRICA

Hlengiwe Dube

Abstract

In contemporary society, technology has become an indispensable facet of childhood experience, with a growing number of children engaging extensively with digital technologies. Despite this pervasive trend, a significant digital divide and exclusion persists, particularly in the African context, primarily attributed to economic disparities, rendering numerous children devoid of internet connectivity and digital resources. For the connected, the digital age has substantially shaped their experiences, yielding both favourable and adverse consequences. The positive impact is evident in the augmentation of their independent development and other benefits stemming from digital engagement. However, this positive trajectory is accompanied by a concerning dimension wherein children, while utilising and deriving benefits from the internet, are increasingly susceptible to exploitation on online digital platforms. As technology becomes increasingly pervasive and sophisticated, children's vulnerability to online harms escalates concomitantly with their engagement in diverse digital technologies. These online risks encompass child grooming, the improper use of personal information, cyberbullying, sexual exploitation, manifestations of depression and anxiety, exposure to inappropriate content, and the ominous threat of child trafficking. Preserving children's privacy in the digital age emerges as a complex challenge with a nuanced interplay between child protection and autonomy. The paradox inherent in child protection and autonomy presents a nuanced challenge. Conventional wisdom holds that parental guidance serves as the conduit for fostering children's well-being and developmental growth. However, the imperative acknowledgment of children's autonomous existence necessitates careful consideration. Despite the prominence of discourse on children's rights in the Global North, such discussions remain relatively novel in Africa, lacking sufficient attention in Africa. This chapter explores the vulnerabilities experienced by children as active participants in the digital age and elucidates the implications for their privacy.

1 Introduction

Digital and mobile penetration rates are on the rise in Africa, coinciding with the continent's embrace of the fourth industrial revolution (4IR).

According to the International Telecommunication Union (ITU), there was a notable 21 percent increase in the deployment of the 4G networks in 2020. Statistics from the same year reveal that 40 percent of the younger demographic, aged 15 to 24, were using the internet.¹ As the surge of internet penetration continues, children and young people now constitute a significant proportion of the interconnected society. These technological advancements wield a profound impact on children's rights.² Notably, children develop a digital identity and digital footprint from very early on, and sometimes preceding their birth.³ This technology evolution is underscored by children's active social media presence where they have profiles, share their experiences, perspectives and other forms of personal information.

The digital space and technology have many attributes that are beneficial to the development of children. Technologies in this regard encompass the internet, artificial intelligence (AI), robotics, big data, algorithms, information, and communication technologies (ICTs). Considering the demographic prevalence of children in the Global South and Africa, a discernible trend emerges, suggesting a potential surge of children as internet users and assuming a dominant role in shaping the digital landscape.⁴ The advent of the COVID-19 pandemic and the imposed lockdowns in response to the pandemic prompted a shift to the digital world and resulted in the escalation of children using digital technologies for recreational and education purposes. Their screen time increased significantly, notwithstanding their limited knowledge of and skills for ensuring their online safety. The United Nations Children's Fund (UNICEF) underscored the potential risks, noting that 'spending more time on virtual platforms can leave children vulnerable to online sexual

1 International Telecommunication Union 'Measuring digital development: Facts and figures' (2020), <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf> (accessed 16 June 2022).

2 A Third and others 'Recognising children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice' in B Wagner and others (eds) *Research handbook on human rights and technology* (2019) 378. The digital age is contributing significantly to the hurdles that hinder the fulfilment of the rights of the child: privacy complications; discriminatory emerging technologies such as artificial intelligence (AI); novel forms of sexual abuse and exploitation; Networked participation and education; and many more.

3 United Nations Human Rights Office of the High Commissioner 'Children's right to privacy in the digital age must be improved' (15 July 2021), <https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved> (accessed 15 March 2022). Parents or other family members share their images on online platforms.

4 Third and others (n 2) 376.

exploitation and grooming'.⁵ In contrast to Europe, the United States and Canada, most African countries exhibit a comparatively lesser emphasis on issues related to child online safety.

Children engage with a myriad of digital technologies including virtual assistants, wearable devices, smartphones, and interactive toys, thereby significantly influencing their childhood, both positively and negatively. This integration of technologies into their lives fosters their participation, augments learning outcomes, enhances access to information, facilitates social interaction, and also recreational purposes. This multifaceted role of technology in children's experience enables them to explore their creativity and empowers them to freely express themselves. Notably for children with disabilities, technology emerges as a mechanism for dismantling, providing them an avenue to access education among other benefits. However, as children navigate a digitised world and interact with technologies, they are exposed to inherent risks and potential harms that could be detrimental to their well-being and undermine their ability to fully harness the advantages of a networked world.

Children are exposed to violence, harmful and inappropriate content, and manipulation of their personal information.⁶ The harmful content encompass that of a sexual nature, non-consensual engagements such as sexting, instances of online sexual abuse and harassment and cyberbullying.⁷ Also, in the cyberspace, children are susceptible to radicalisation and exploitation by non-state actors such as terrorist groups and extremists. Through these liaisons, children are prompted to engage in detrimental behaviours including acts of violence.⁸ Children may also use technology to utter proclamations that disparage or denigrate others based on unique aspects of their individuality or collective identity such as sexual orientation, religion, nationality, race, economic background, political affiliation, ethnicity and sex/gender. They may also generate or disseminate malicious or spiteful content targeted at particular demographic categories.

5 UNICEF 'Children at increased risk of harm online during global COVID-19 pandemic – UNICEF' (20 April 2020), <https://www.unicef.org/southafrica/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic-unicef> (accessed 16 June 2022).

6 IR Berson & MJ Berson 'Children and their digital dossiers: Lessons in privacy rights in the digital age' (2006) 21 *International Journal of Social Education* 136.

7 Third and others (n 2) 378. '[T] he internet is generally designed for adults ... the internet is age-blind.'

8 General Comment 25 para 83.

The digital and data economy has undergone exponential growth, resulting in substantial personal information being stored in digitised formats.⁹ This underscores the aforementioned vulnerability of children considering their limited knowledge and capacity to control the processing of their personal information. A significant volume of their data is being processed, including collection, storage, transfers and re-purposing, without their knowledge or informed consent. In the African context, data protection mechanisms are still nascent, however, this immature and transitional phase children's vulnerabilities are exacerbated. The right to privacy is a fundamental right that is enshrined in international human rights law and standards. It is not an absolute right and any interference should be proportionate, legitimate, necessary and serve a legitimate purpose. In addition to this international law position, any limitations to children's privacy should be consistent with the principle of data minimisation and prioritise the best interests of the child.¹⁰

The challenges faced by children infringe on their rights that are enshrined in international human rights law and standards. Ample international human rights instruments and other standard setting documents address children's rights and can also be applied to the digital context. Prominent among these are the United Nations (UN) Convention on the Rights of the Child (CRC)¹¹ and the African Charter on the Rights and Welfare of the Child (African Children's Charter),¹² serving as the main instruments codifying children rights in Africa. Specifically, on the digital age, UN General Comment 25 on children's rights in relation to the digital environment elucidates the implementation of the CRC and its optional protocols in a digital context. It further provides guidance to ensure compliance with obligations on children's rights.¹³ The African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee) also adopted a resolution on the protection and promotion of children's rights in the digital sphere within the African context.¹⁴

9 Berson & Berson (n 6) 136.

10 See General Comment 25 para 69.

11 United Nations Convention on the Rights of the Child, <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> (accessed 15 March 2022).

12 African Charter on the Rights and Welfare of the Child, adopted in 1990 and came into force in 1999, <https://au.int/en/treaties/african-charter-rights-and-welfare-child> (accessed 15 March 2022).

13 General Comment 25 on Children's rights in relation to the digital environment, <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation> (accessed 17 March 2022).

14 African Children's Committee 'Resolution on the Protection and Promotion of

The objectives of this chapter are twofold. The first objective is to highlight the risks encountered by children in online engagements. The second objective is to underscore the intricate privacy conundrum inherent in children's digital interactions. Central to the overarching argument of this chapter is the contention that children's privacy in the digital environment constitutes a critical concern meriting earnest consideration. However, children's privacy should be evaluated from a broader perspective of the digital space that is riddled with hazards that threaten their safety and privacy. In examining the obligations of states, the efficacy of the existing legislation is examined. The initial segment of the chapter examines the vulnerability of children in the digital environment, while the second part considers the privacy aspect, exploring the diverse ways in which the digital environment impacts children's privacy. The third part examines the existing legal frameworks and practices for child protection and privacy. Subsequently, the chapter considers commendable practices from other contexts and examines selected approaches that Africa could potentially adopt. The chapter concludes with proposed recommendations and conclusions designed to enhance online safety of children and enhance their privacy in the African context.

2 Digital risks encountered by children in the digital age

This segment explores the digital risks confronted by children in the digital environment. The focus on the online risks is important as any discourse on children's privacy should also take into account the inherent harms associated with the digital environment, which necessitates a delicate balance between privacy and protection. The digital space has ushered in new avenues for perpetrating violence against children, resulting in dual violation of their rights, both offline and online.¹⁵ Children are also susceptible to online predatory behaviour by online abusers, who are either their peers or adults.¹⁶ Violence against children online manifests in physical and emotional forms and examples include sexual abuse and exploitation, cyberbullying, and the abuse of personal information. Notably, during crisis episodes such as pandemics, networked children's online presence increases and the risk of harm online also escalates.¹⁷

Children's Rights in the Digital Sphere in Africa' (17 March 2022), <https://drive.google.com/file/d/1WhBF7HGfvyTyxWJmkGsHuavnJhZMrDdd/view> (accessed 15 March 2022).

15 Berson & Berson (n 6) 142. See also General Comment 25 para 80.

16 African Children's Committee (n 14).

17 General Comment 25 para 80. In response to changes brought about by the COVID-19 pandemic, the African Children's Committee noted that 'countries have adapted to digital learning methods and this may expose children to online child

These risks can ‘severely harm their mental and emotional health and physical well-being’ and limit a child’s development and also potentially affect their adolescence and adulthood.¹⁸ The risks under consideration are related to conduct, content and contact, each impacting on children’s safety and privacy.

2.1 Cyberbullying

Exposure of children to bullying is not novel and they experience it as either victims or perpetrators. This chapter considers cyberbullying, denoting bullying which occurs through electronic means.¹⁹ Considered as one of the main threats to children in the digital sphere, cyberbullying may be perpetrated by and among children themselves.²⁰ Cyberbullying is linked to the way children conduct themselves online, with other children or adults. It can manifest in the use of digital technologies including social media, instant messaging, email or texts, to propagate hurtful behaviour. It involves sending images such as pictures and videos with insults, false information or threats about the targeted victim who may either be included or excluded from the communication. The behaviour can be once-off or recurrent and is necessitated by an existing ‘power imbalance between the perpetrator and victim’.²¹ Notably, there is a correlation between online and offline cyberbullying, wherein offline incidents and behaviours could migrate to the online space to victimise other children.²² Due to the electronic medium, cyberbullying has an extensive audience and reach, magnifying its impact.²³ Its consequences can be tragic and there is a higher propensity for victims of cyberbullying contemplating

sexual exploitation and abuse’. See African Children’s Committee ‘Guidance note on children’s rights during COVID-19’ (8 April 2020), <https://www.acerwc.africa/guiding-note-on-childrens-rights-during-covid-19/> (accessed 18 March 2022). See also African Children’s Committee (n 14).

18 OHCHR (n 3).

19 RR Calvoz and others ‘Constitutional implications of punishment for cyber bullying’ (2014) *Cardozo Law Review* 105.

20 MG Vallejo and others ‘Kids and parents privacy exposure in the internet of things: How to protect personal information?’ (2018) 22 *Computación y Sistemas* 1196.

21 UNICEF M Stoilova and others ‘Investigating risks and opportunities for children in a digital world’ (February 2021) 38, <https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf> (accessed 5 April 2022).

22 Stoilova and others (n 21) 39.

23 R Slonje & PK Smith ‘Cyberbullying: Another main type of bullying?’ (2008) 49 *Scandinavian Journal of Psychology* 147-154.

suicide.²⁴ Although there are no figures for South Africa, there is a significant occurrence of cyberbullying among children in the country.²⁵

Cyberbullying exhibits gender-specific variations, with a higher probability of boys being perpetrators and girls being victims.²⁶ Girls are often targeted on the basis of their physical appearance or sexuality, thereby exerting a profound impact on their reputation and dignity. Such consequences may potentially exacerbate their vulnerability to social exclusion and escalate or perpetuate the ongoing abuse.²⁷ Due to the appearance based focus, social media becomes a predominant channel for girls' harassment. Conversely, boys experience cyberbullying differently, often associated with playing video games and messaging via mobile phones.

Several factors contribute to the occurrence of cyberbullying including perceptions around violence, a lack of empathy, an exaggerated sense of self-importance and desire for popularity, and diminished self-efficacy tendencies.²⁸ Vulnerable demographics such as children of single parents, those with disabilities, those who suffer from social anxiety and those from economically disadvantaged school backgrounds are more susceptible to online bullying.²⁹ The protection landscape against bullying is increasingly becoming more complex. For instance, a child's home usually was their traditional place of safety where they could evade school or neighbourhood bullies. However, in the digital realm, exacerbated by the proliferation of social media presence, bullies transcend the physical barriers of protection, leaving victims without places of solace.³⁰

In the context of cyberbullying, the issue of privacy is notably intricate given the possibility of cyberbullying occurring in anonymity or facilitated by use of stolen identities, posing substantial complications to formulating interventions to remedy the victims' situation.³¹ In this conundrum, the elusive nature of cyberbullying intensifies the possibility of privacy infringements for the victims due to their susceptibility to

24 M Laubscher & WJ van Vollenhoven 'Cyberbullying: Should schools choose between safety and privacy?' (2015) 18 *Potchefstroom Electronic Law Journal* 2219.

25 As above.

26 Stoilova and others (n 21) 39.

27 As above.

28 As above.

29 As above.

30 UNICEF 'The state of the world's children 2017: Children in a digital world' (2017) 21, <https://www.unicef.org/media/48601/file>.

31 Laubscher & Van Vollenhoven (n 24) 2234.

unwarranted exposure, particularly concerning sensitive information, further compounding the challenges associated with finding solutions to mitigate the far-reaching impact of cyberbullying.

2.2 Exposure to inappropriate content

The content under consideration encompasses discriminatory, sexual, pornographic, hateful, violent or racist expressions. This kind of content can also depict certain behaviours that are detrimental to the well-being of children including instances of self-harm, suicide, eating disorders, gambling, hacking, as well as hurtful and bullying behaviour.³²

2.3 Sexual risks and Exploitation

Children are increasingly exposed to various sexual activities in the digital space, including engaging in cybersex, and the consumption or exchange of sexual content.³³ Concurrently, the digital environment also exposes them to sexual abuse and exploitation. Cyber sexual exploitation and abuse, a manifestation of digitally-facilitated child sexual abuse entails generating and disseminating child sexual abuse materials; child prostitution; solicitation of sexual acts from minors; threats to a child's reputation; bullying; and the encouragement of children to engage in self-harming behaviours such as suicidal tendencies.³⁴ Such malevolent acts, typically perpetrated by online sex predators, stem from exploitation of trust established in interactions with minors online. Another disconcerting and prevalent manifestation is online intimate partner violence, a technology-assisted form of violence that manifests in forms of control such as harassment and stalking in the context of a friendship or a pre-existing relationship. Notably higher prevalence of this form of violence is exhibited among teenage girls.³⁵

2.4 Exchange of sexual content (sexting)

Sexting is the exchange of sexually explicit content including videos, messages and images through internet-based platforms or mobile phones. While sexting is not inherently risky and can be consensual. It is normal and common behaviour associated with a child's development, particularly during adolescence. At this stage, teenagers engage in sexting as they explore relationships and their sexuality. The initiation and

32 UNICEF (n 30).

33 Stoilova and others (n 21) 45.

34 General Comment 25 para 81.

35 Stoilova and others (n 21) 56.

frequency depends on the child's socio-economic status, age, gender and sexual orientation. It is common among teenagers in general and more prevalent among those in the lesbian, gay, bisexual, trans and gender diverse, intersex and queer (LGBTIQ) demographic. Also, the inclination to coerce partners to share sexual content is more pronounced among older children, particularly boys, as compared to the younger ones.³⁶

While it is common in digital communication, sexting is inherently associated with risks that include non-consensual transmission of sexual content, sexual bullying harassment and non-consensual dissemination of intimate information.³⁷ The probability of girls having negative experiences arising from sexting is high, whereas boys' vulnerability is lower.³⁸ Risks associated with children's experiences while exchanging sexual content online include privacy infringements; compromised online safety; sexual solicitations by adults; sexual grooming; and adverse psychological consequences.³⁹ For instance, non-consensual sharing of images has detrimental effects on the victim's privacy and reputation, often culminating in stigmatisation or slut-shaming.⁴⁰

2.5 Viewing sexual content online

Engaging with sexual content online involves consumption of sexually-explicit videos or images. Such exposure could be intentional or accidental, with a prevailing curiosity rooted in the quest for sexual knowledge.⁴¹ Notably, there are gender disparities with boys exhibiting more interest in this type of content compared to girls. Although parental involvement can shield children from such exposure, children can circumvent parental control barriers to gain access to explicit content. Additionally, children also exhibit deceptive tendencies and falsify their age information to enable them to access content that is not age-appropriate for them.⁴² The ramifications for such exposure, includes engaging in sexting with strangers or unwarranted sexual solicitation by strangers.⁴³ Consequences

36 Stoilova and others (n 21) 46.

37 Stoilova and others (n 21) 45.

38 As above.

39 Stoilova and others (n 21) 45.

40 Stoilova and others (n 21) 46.

41 Stoilova and others (n 21) 48.

42 Pew Research Centre A Lenhart and others 'Teens, kindness and cruelty on social network sites' (9 November 2011) <https://www.pewresearch.org/internet/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/> (accessed 26 June 2022).

43 Stoilova and others (n 21) 48.

are multifaceted and extend beyond the digital sphere, manifesting as psychological effects, social withdrawal during internet disconnection and occasional sleep disturbances.⁴⁴

2.6 Contact with online predators

Online predators adeptly assume deceptive personas and strategically target online platforms commonly accessed by children. The initial encounter with the perpetrator could be either online or conventional offline interactions.⁴⁵ Predators establish interactions with minors and cultivate illusions of genuine friendships to foster a sense of trust. There is a perilous possibility of online liaisons culminating in in-person relationships.⁴⁶ In these orchestrated liaisons, there is a risk of minors being manipulated into divulging sensitive personal information, including contact details and location data. This surreptitious exchange of information often transpires without the parents' knowledge, thereby impeding their ability to protect their children from potential online threats including those posed by predatory individuals. The prospect and nature of exploitation are contingent upon factors such as a child's age, socio-economic background, gender, and other pertinent considerations.⁴⁷

Online predators manipulate minors to perform sexual acts online.⁴⁸ The exposure of children to offline or online abuse, orchestrated by adults or their peers could propel them to engage in more risky activities including communicating with strangers and sharing personal information. Also, children's immersion in online platforms and the nature of their liaisons could potentially steer them towards exploring sexual activities that expose them to abuse and exploitation.⁴⁹ Older adolescent girls are more predisposed to victimisation as compared to younger ones, both girls and boys.⁵⁰ Additionally, LGBTIQ minors are also susceptible to such risks. While parental guidance and mediation play a crucial role in assisting victimised children, the efficacy of this intervention may be undermined by children's failure to recognise the precarious nature of their situation and consequently refrain from seeking the requisite assistance.⁵¹

44 As above.

45 As above.

46 General Comment 25 para 81.

47 As above.

48 As above.

49 Stoilova and others (n 21) 51.

50 Stoilova and others (n 21) 50.

51 As above.

2.7 Online sexual solicitation of children (child grooming)

Online sexual solicitation of children, commonly referred to as grooming, involves the establishment of inappropriate offline and online relationships between a minor and an adult for the purposes of sexual conduct.⁵² This form of child exploitation manifests in various forms including coaxing children to engage in sexual acts or share personal sexual information in virtual platforms such as social media, email or through texting.⁵³ Predominantly, the targeted children exhibit behaviours such as intense involvement in online gaming, forming friendships with strangers, consuming sexually explicit content, oversharing personal information on the internet, willingly participating in sexting, particularly with strangers, and generally spending extensive periods online, especially during weekends. Notably, a correlation exists between online and offline vulnerabilities, wherein perpetrators may either be acquainted with their online targets or, more commonly, remain strangers.⁵⁴ Children who have experienced offline abuse, encompassing sexual exploitation, neglect, physical punishment, or psychological torment, demonstrate an increased susceptibility to succumb to online sexual solicitation.⁵⁵ It is crucial to acknowledge the role of social support in mitigating the impact of such abuse, as those lacking such assistance face heightened vulnerability, leading to potential self-harm.

2.8 Sextortion

This involves coercive threats of disseminating sexual images without the owner's consent, is a common issue driven by motives associated with revenge or financial gain and it primarily manifests in pre-existing relationships or friendships. Sextortion exhibits a notable prevalence of male involvement, whether as victims or perpetrators. Furthermore, empirical evidence suggests a disproportionate impact on non-heterosexual individuals, irrespective of their age or racial background.⁵⁶

This section of the chapter extensively explores the adversities confronted by children in their digital experience. As succinctly conveyed by Bush, 'kids are too immature to deal with blackmail, extortion, revenge porn, stalking, being hounded down for nudes, cyberbullying,

52 African Children's Committee General Comment 7 para 70. Child sexual online grooming is common among children between 13 and 17 years of age, mainly girls.

53 Stoilova and others (n 21) 51.

54 Stoilova and others (n 21) 52.

55 As above.

56 As above.

being socially excluded, and so much more. Kids can't deal with these issues in the real world, let alone the online world.'⁵⁷ The contention posited is that, owing to their inherent immaturity, children struggle to navigate these complex issues in both the physical and digital spheres. The subsequent discussion underscores the intrinsic link between these digital perils and the erosion of trust in technology, thereby prompting parental intervention to safeguard their children. This encroachment on the private online domain of minors is scrutinised in the subsequent segment of this chapter.

3 Privacy implications of children's interaction with technology in Africa

As previously indicated, internet connectivity has significantly improved in Africa, thereby facilitating increased access to social media. Consequently, heightened consideration is warranted for the privacy discourse, given the implications of internet connectivity, particularly concerning children, a focus that has received comparatively less attention.⁵⁸ In Africa the discourse on privacy is gaining traction but still is at nascent stages and yet to attain full societal recognition. The inherent complexity of technology, coupled with the omnipotence of technology-based innovations, undermines individuals' ability to exercise adequate control over their personal information and protect their privacy.

Information processing has evolved significantly, advancing in sophistication and occurring at unprecedented speeds. Additionally, the digital ecosystem is predicated on continuous user monitoring and data processing, presenting an imminent threat to privacy. This transformation is enabled by the emergence of big data and other emerging technologies that facilitate the processing of vast datasets through intricate mechanisms designed for the storage, analysis, and manipulation of information. These technological advancements find application in diverse domains such as surveillance, marketing, and profiling.

57 N Bush 'Cyberbullying, social media and compulsive gaming' (24 March 2022) *IOL*, <https://www.iol.co.za/the-post/features/cyberbullying-social-media-and-compulsive-gaming-38e6ca99-f507-4865-91d4-57ebd0d0643c> (accessed 26 June 2022).

58 K Goldstein 'I'm a mom and a children's privacy lawyer: Here's what i do and don't post about my kid online' (17 May 2022), <https://www.parents.com/kids/safety/internet/im-a-mom-and-childrens-privacy-lawyer-what-i-do-and-dont-post-online/> (accessed 12 April 2022).

The digital lifestyles entail documenting and sharing experiences and information, extending to the context of children.⁵⁹ Also, in contemporary networked societies, routine practices include mandatory identity verification, mass surveillance,⁶⁰ profiling, automated data processing, behavioural targeting, and filtering are now ordinary practices.⁶¹ Beyond the realm of families sharing information, public and private institutions actively process children's information. The processed information includes children's emotions, activities, location, relationships, identities, communication, academic performance, gender, race, health and biometric data, all of which can uniquely identify them. This processing is undertaken for purposes related to education, health, and various other societal considerations.⁶²

There is a correlation between privacy and the digital risks that have been articulated. Privacy intrusions can impact negatively on the identity and reputation of individuals. Generally, children are not concerned about their digital footprint and the privacy implications in comparison to adults. Consequently, there is a tendency for lower levels of privacy management and the implementation of safety strategies among children. While possessing some requisite skills, children may not consistently apply them.⁶³ It is imperative to redirect attention towards enhancing privacy management and fostering media and digital literacy among the younger demographic. The illicit processing of information is an indisputable reality, imperilling the privacy of children, a domain that should be held as sacrosanct as that of adults. Of particular concern is the manipulation and non-consensual dissemination of information.

59 J Gligorićjević 'Children's privacy: The role of parental control and consent' (2019) 19 *Human Rights Law Review* 202.

60 See General Comment 25 para 75, which states that obligations on mass surveillance and children's privacy require that '[a]ny digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose'. In the case of tracking devices and monitoring a child's digital activities, such measures should take into account the evolving capacities of the child, serve the best interests of the child and proportionate. See para 76 General Comment 25.

61 General Comment 25 para 68.

62 General Comment 25 para 67. Eg, state and private sector surveillance and transactional data collected by commercial actors. See Third and others (n 2) 387.

63 Stoilova and others (n 21) 31. As a result of their higher levels of vulnerability, girls are more likely to be concerned about their privacy and adopt better privacy behaviour than boys.

Although considerable progress has been made in interpreting the right to privacy, the inclination in the context of children tends to prioritise parental control and child protection, which overshadows the imperative of safeguarding the child's privacy.⁶⁴ Globally, incidents of online risks and privacy infringements against children have become prevalent, necessitating an augmented call for prompt intervention.⁶⁵ This section of the chapter delves into pivotal facets of privacy in children's online information, encompassing parental responsibility, the phenomenon of "sharenting"; children's online behaviours that pose risks to their privacy; the conundrum of privacy and data protection in the education sector; and the privacy ramifications arising from the advent of emerging technologies such as artificial intelligence (AI).

3.1 Parental guidance in relation to child autonomy and privacy

Parental responsibility is a recognised mechanism that chaperones children throughout their development stages. It includes a broad spectrum of roles such as providing guardianship, care, offering the necessary support and maintaining contact and communication with the child. According to Du Toit, 'parents are key parts of the immediate "eco-system" of a child and are critical in a healthy development of the child, including the functioning and progress of the child'.⁶⁶ The concept of parental responsibility is recognised under international human rights. Article 5 of CRC states:⁶⁷

States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

Although privacy is a fundamental right, it is not absolute and can be limited. In the context of children, parental responsibility emerges as a potential limiting factor; however, the precise extent of this limitation remains ambiguous. Striking an optimal balance between a child's autonomy and parental responsibility is imperative to prevent parents and guardians from

64 Gligorijevic (n 60) 202.

65 Third and others (n 2) 391-403.

66 T du Toit 'Cyber bullying dilemma: A case for ubuntu', '<https://rm.coe.int/cyberbullying-dilemma-a-case-for-ubuntu-by-thersia-du-toit-smit-nation/1680a30051>' (accessed 18 June 2022).

67 Art 5 CRC; also arts 3, 18 & 19.

exerting absolute control that could impede the child's developmental trajectory. When courts adjudicate matters pertaining to a child's privacy, it becomes essential to elucidate the impact of parental behaviour on the child's privacy. This should be done without reproaching parents for their parenting choices or positioning courts as moral adjudicators arbitrating what constitutes commendable or acceptable parenting practices.⁶⁸

Parental responsibility should be exercised with unwavering commitment to the best interests of the child, a cardinal principle underpinning the safeguarding and advancement of children's rights.⁶⁹ In the context of children's privacy within the purview of parental responsibility, there seems to be a *lacuna*. It is generally recognised that children cannot be left entirely to navigate their developmental journey autonomously. Justifiable limitations on their autonomy are crucial to shield them from potential harm, whether directed towards others or themselves.⁷⁰ In this regard, as children increasingly access the online sphere, parents assume a 'supervisory and guardianship role'.⁷¹ This is an indispensable role for regulating a child's digital lifestyle, mitigating the risks of online harms. Parental involvement assumes paramount importance, facilitating a nuanced understanding of their children's online behaviour and offering requisite guidance when feasible.⁷² This form of surveillance has become an integral aspect of contemporary parenting in the digital age.

There is a genuine concern for the safety of children that drives parents to infringe on children's privacy and monitor their digital habits.⁷³ As highlighted earlier, children are susceptible to cyberbullying, exposure to inappropriate content, and exploitation by online predators, including incidents of sexual abuse. Additionally, children may utilise digital channels to engage in illicit behaviour such as drug distribution and

68 Gligorijevic (n 60) 205.

69 Art 3 CRC.

70 Laubscher and Van Vollenhoven (n 24) 2231.

71 Humanium 'Children's rights and digital technologies: Children's privacy in the age of social media – The perils of "sharenting"' (26 January 2021), <https://www.humanium.org/en/childrens-rights-and-digital-technologies-childrens-privacy-in-the-age-of-social-media-the-perils-of-sharenting/> (accessed 26 June 2022).

72 MacAfee 'America's youth admit to surprising online behavior, would change actions if parents were watching' (4 June 2013), <https://www.businesswire.com/news/home/20130604005125/en/America%E2%80%99s-Youth-Admit-Surprising-Online-Behavior-Change> (accessed 26 June 2022).

73 C Null 'I monitor my teens' electronics, and you should too' (27 January 2020) *WIRED*, <https://www.wired.com/story/parents-should-monitor-teens-electronics/> (accessed 20 June 2022).

organising of gathering with explicit sexual content, commonly referred to as sex parties. Parents perceive these as serious concerns, thus superseding considerations of privacy. The capacity of children to make regrettable decisions online underscores the necessity of employing monitoring applications and devices as essential tools for ensuring their safety and potentially saving lives.⁷⁴

The paramount motivation behind the monitoring of children's online and offline activities is the ardent desire to safeguard them from potential harm in the digital realm. The perils associated with children's digital experiences have been extensively elucidated in the preceding section of this chapter. Parents and caregivers, grappling with an inherent ambivalence towards the digital space and the myriad risks it poses to children, are inclined towards privacy-intrusive behaviours and heightened restrictions.⁷⁵ Parents feel that they have effectively exercised their duty to care in the digitised world when they monitor their children's online activities. The online monitoring is perceived as an extension of the vigilant supervision exercised in offline settings. Consequently, parents find assurance in the belief that they have fulfilled their moral responsibility, thereby ensuring the safety and well-being of their children.

The digital sphere introduces an additional layer of vulnerability for children, particularly those who are already susceptible, such as those with disabilities. For these children, the access and utilisation of assistive technology signify a transformative experience, rendering achievable what would otherwise be deemed unattainable. The heightened vulnerability of children with disabilities in the digital sphere requires proactive engagement and parental support or those with parental responsibility. For instance, for visually-impaired children, reading social cues could be challenging. Children with intellectual and psychosocial disabilities may encounter the challenge of making appropriate judgments.⁷⁶ Moreover, children with albinism generally encounter life-threatening victimisation, such as organ harvesting, a peril that extends to their digital life where they may be targeted by predators. This unique position of children with disabilities in the digital age mandates assisted use of technologies. In undertaking this role, there is the inevitability of encroaching into the child's private space. Effectively managing the vulnerability and disability intersectionality with a child's privacy during the assisted use of technologies becomes a

74 As above.

75 Third and others (n 2) 392.

76 C Kagwiria 'Child online protection for children with disabilities' (10 December 2021), <https://www.afralti.org/child-online-protection-for-children-with-disabilities/> (accessed 5 April 2022).

nuanced and delicate task. It is therefore imperative to employ thoughtful approaches to parental guidance, ensuring autonomy, safety and dignity of these children.

Parents use digital and non-digital means to conduct overt or covert surveillance on their children's digital presence. This surveillance extends to monitoring their networking, messaging and browsing history.⁷⁷ The expectation of privacy further diminishes when the child uses their parent device, a common scenario in the African context. Such devices are the parent's property, which they routinely inspect. Non-digital monitoring methods include temporary sequestering of children's devices to regulate their screen time and concurrently scrutinise their children's online activities.

Technologies have been developed to enable parents to remotely clone their children's devices and monitor their online behaviour. An example is the Life360 application which offers real-time monitoring of capabilities, including the ability to assess device battery levels and driving speeds.⁷⁸ Parents employ these monitoring technologies to not only regulate screen time but also enforce content restrictions, thereby minimising exposure to inappropriate content. Additionally, digital surveillance cameras are also installed in homes to monitor children and sometimes their helpers. The prevalence of technology monitoring extends beyond home settings to educational institutions such as schools and play centres, where it serves as a proactive measure to mitigate security risks.⁷⁹ At play centres, for instance, parents can observe their children engaging in various activities and establishing friendships. Notably, the installation of surveillance cameras has become a norm in South African nursery schools and child care centres due to the unfortunate occurrence of child abuse incidents in these institutions.⁸⁰ The priority is placed on parental surveillance and the consent of the parent serves as justification for parental intrusions into the child's privacy.

77 K Mathiesen 'The internet, children, and privacy: The case against parental monitoring' (2013) 15 *Ethics and Information Technology* 263-264.

78 J Keegan & A Ng 'The popular family safety app Life360 is selling precise location data on its tens of millions of users' (6 December 2021) *The Markup*, <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user> (accessed 20 June 2022).

79 Berson & Berson (n 6) 138-140.

80 'Something to ponder: Surveillance cameras to protect our children' (2019) *iAfrica*, <https://iafrica.com/something-to-ponder-surveillance-cameras-to-protect-our-children/> (accessed 26 June 2022).

The deployment of monitoring practices has implications on the child's privacy. For instance, the infringement into the child's privacy extends to the child's contacts, primarily composed of children too, and would not have consented to processing of their information by a third party, including communications.⁸¹ Also communications between children take place in the context of friendship, with an expectation of privacy in that relationship.

Parental monitoring presents challenges to children in unique circumstances that require greater levels of privacy. This is particularly pertinent for children experiencing abusive home environments, adolescents seeking autonomy, and those identifying with sexual minorities, as well as individuals in stringent religious communities. In such instances, these children aspire to explore their choices, identities, and circumstances discreetly, avoiding potential embarrassment or surveillance by their parents.⁸² Privacy emerges as a critical factor for children with diverse gender and sexual orientations, including trans and queer teens, who rely on it to navigate the intricate process of self-discovery and, eventually, confidently disclose their identities to the public. The imposition of parental surveillance may impede or altogether thwart this exploratory journey. A child's exploration of their identity, manifesting through web searches indicative of being lesbian or gay, may result in harm, particularly for those whose parents harbour strong convictions against individuals with diverse sexual orientations.⁸³

In the context of adolescent development, older teenagers may find themselves seeking access to sensitive health-related information pertinent to intimate aspects of their growth. Such inquiries may pertain to matters they are hesitant to discuss with their educators or parents and guardians. Sensitive health information may be collected and processed through online counselling services. Consequently, it becomes imperative for counselling service providers to maintain high standards of confidentiality and data protection. Stringent privacy safeguards should be implemented to govern the handling of information within online counselling platforms. An alternative approach may involve considering an exemption for online counselling services from the mandate requiring parental consent.⁸⁴

81 C Harrell 'The kid surveillance complex locks parents in a trap' (20 December 2021) *WIRED*, <https://www.wired.com/story/the-kid-surveillance-complex-locks-parents-in-a-trap/> (accessed 26 June 2022).

82 Third and others (n 2) 145.

83 Mathiesen (n 78) 268.

84 General Comment 25 para 78.

The pervasive ownership of monitoring applications by companies has resulted in the extensive collection of children's personal information, often lacking essential safeguards to protect such data from potential misuse. Unfortunately, a considerable number of parents remain uninformed about the privacy policies of these companies, some of which explicitly disclose the sharing or sale of data to third parties. The primary focus of parents tends to be on monitoring activities, with a lack of awareness or prioritisation of potential consequences, such as data brokering. Notably, owners of monitoring applications engage in the sale of children's location and other sensitive data to data brokers. For instance, applications like Life360 accumulate location data for children and their families without implementing adequate measures for ensuring the integrity and confidentiality of information security.⁸⁵

Day care centres' use monitoring applications that allow parents to remotely monitor or observe children, raise concern given the risks associated with data collection and sharing when fundamental information security practices and privacy considerations are not accorded due priority. Issues such as securing public cloud buckets hosting children's data, implementing robust cloud server images, embracing end-to-end encryption, and enforcing two-factor authentication become pivotal in mitigating potential risks.⁸⁶ The deficiency in proactive disclosure pertaining to information-sharing practices with third parties exacerbates the concerns. There exists a plausible scenario wherein information concerning these preschoolers may be disseminated on social media platforms, such as Facebook, without requisite parental or guardian consent.⁸⁷ While the convenience of the monitoring and observation application provides parents with a reassuring sense of remote child monitoring, it concurrently disregards the legitimate concerns surrounding unauthorised access to and utilisation of their child's information by third parties. In the South African context, privacy apprehensions persist despite the perceived security benefits offered by day care centres and camera surveillance. Furthermore, the sharing of passwords used by parents to log into nursery schools or day care facilities with external individuals compounds these privacy concerns.⁸⁸ The convenience of the monitoring and observation application affords parents a reassuring sense of ease as they remotely supervise their children. However, this convenience

85 Keegan & Ng (n 79).

86 A Hancock 'Parents need to know what's going on inside their day care apps' (23 June 2022) *WIRED*, <https://www.wired.com/story/daycare-app-privacy-security/> (accessed 20 June 2022).

87 As above.

88 As above.

supersedes any apprehensions related to possible unauthorised access and use of their child's information.⁸⁹

There are views that there should be a focus shift directing more attention towards developers of inappropriate content that children may encounter online, instead of monitoring children online.⁹⁰ While there is merit in this approach, it is much more complex, exceeding the monitoring capabilities of parents themselves. Drawing on Zuboff's insights, practising surveillance on children contributes to the proliferation of surveillance capitalism profiting corporations.⁹¹ Parents are incentivised to buy surveillance devices that enhance the safety of their children online. Zuboff contends that the intensified culture of monitoring stems from a trust deficit towards children by parents, which fosters a climate of suspicion and cultivates the acceptability of the privacy infringements among the younger demographic.

Another oppositional position to monitoring of children's online behaviour is propagated by Mathiesen, who contends that such parental surveillance is paternalistic and deemed 'ethically inappropriate'.⁹² Mathiesen advocates for prioritising children's rights to privacy over justifications for parental monitoring.⁹³ Mathiesen's assertion is underpinned by two crucial two positions. Firstly, Mathiesen argues that 'privacy is necessary in order to respect children's current capacities for autonomy and to foster their future capacities for autonomy'.⁹⁴ Secondly, 'privacy is necessary in order to protect children's current capacities for relationships and to foster their future capacities for relationships, this includes their developing the capacity to trust, and be trustworthy'.⁹⁵ However, this paramountcy of privacy is not absolute. In instances where the necessity to protect the children is presented, the obligation to protect takes precedence and overrides privacy considerations.⁹⁶

89 Creche and Nursery Schools for South Africa 'Day-care with cameras', <https://creche-nurseryschools.co.za/day-care-with-cameras/> (accessed 20 June 2022).

90 Harrell (n 82).

91 See generally S Zuboff *The age of surveillance capitalism* (2019).

92 Mathiesen (n 78) 263-264.

93 Mathiesen (n 78) 267.

94 Mathiesen (n 78) 269.

95 As above..

96 Mathiesen (n 78) 271.

The exercise of parental responsibility demands a nuanced distinction between monitoring for protection and intrusive interference.⁹⁷ While there is justifiable focus and emphasis for child safety in the digital age, it should be acknowledged that privacy is also important for children's dignity; autonomous development and general psychosocial well-being; their agency, and the general exercise of their rights.⁹⁸ It is the anonymity and the ability to operate in private that afford children the opportunity to explore and define their identity and exercise self-determination without being subjected to unwarranted exposure or surveillance compromising their privacy.⁹⁹ Also, privacy enables them to cultivate friendships and relationships, integral components of normative child development. Therefore, incursion into privacy should be executed with meticulous consideration and guided by the imperative to shield a child from harm.¹⁰⁰ According to Mathiesen, striking the delicate equilibrium between protecting children from online threats and respecting their privacy entails fostering parent-child interactions that educate children and equip them with the necessary skills to navigate digital challenges.¹⁰¹ Engaging in such conversations also encourages children to openly discuss their struggles within the digital environment.

3.2 Parents' actions that expose children's personal information

3.2.1 Sharenting

Another aspect that presents complexities in children's privacy is the practice referred to as 'sharenting'. It takes diverse forms, ranging from online diaries chronicling a child's journey to the general dissemination of videos and photographs, and even the establishment of social media

97 C Popa 'Controlling children's passwords is a flagrant breach of their privacy' (27 August 2020) *The Conversation*, <https://theconversation.com/controlling-childrens-passwords-is-a-flagrant-breach-of-their-privacy-141031> (accessed 26 June 2022).

98 General Comment 25 para 67.

99 General Comment 25 para 77. 'Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyber aggression, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.'

100 Mathiesen (n 78) 271.

101 Mathiesen (n 78) 272.

accounts dedicated to children.¹⁰² The information is shared either with close family and friends or with a broader digital network.¹⁰³ Sharenting is facilitated by power dynamics inherent in child-parent relationships, particularly in early childhood when parents wield absolute control and authority over the child's information. At that stage, cognitively, children lack the capacity to comprehend the intricacies of their lives, including consent.¹⁰⁴ In this context, the emphasis on the child's individual autonomy and control is notably diminished. Sharenting results in digital documentation of children's lives on digital platforms, coining the term 'generation tagged' to describe this prevalent reality.¹⁰⁵ Consequently, children reach adulthood with an already developed digital identity and footprint.¹⁰⁶

Motivational factors behind sharenting include perceived benefits such as creating memories, updating family and friends and sharing parental experiences or soliciting for support in the parental journey.¹⁰⁷ However, despite these benefits, there are privacy implications.¹⁰⁸ The showcasing through sharenting relegates to secondary position pertinent aspects such as dignity and privacy of the child. While some parents may be aware of the privacy risks associated with sharenting and discontinuing the practice, the tendency to share children's images on social media platforms remains prevalent and the trend continues to escalate with the emergence of additional social media platforms and the unprecedented increase of online and social media users.¹⁰⁹

Privacy and digital identity development are at stake when considering the impact of sharenting. The paramountcy of privacy implications heightens, notably at adolescence, a transitional stage when children start development of their independent digital identity.¹¹⁰ When parents

102 K Kopecky and others 'The phenomenon of sharenting and its risks in the online environment: Experiences from Czech and Spain' (2020) 110 *Children and Youth Services Review* 2.

103 Gligorijevic (n 60) 202.

104 Gligorijevic (n 60) 204.

105 E Nottingham 'Sharenting in a socially distanced world' (12 August 2020), <https://blogs.lse.ac.uk/parenting4digitalfuture/2020/08/12/sharenting-during-covid/>.

106 Berson & Berson (nn 6) 141.

107 G Ouvrein & K Verswijvel 'Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management' (2019) 99 *Children and Youth Services Review* 320.

108 As above.

109 E Nottingham 'Sharenting in a socially distanced world' (12 August 2020), <https://blogs.lse.ac.uk/parenting4digitalfuture/2020/08/12/sharenting-during-covid/>.

110 Ouvrein and Verswijvel (n 107) 325.

share content they deem sensitive and inappropriate, it negatively affects their reputation and the digital identity they aspire to cultivate. Also, the ‘permanence of online information’ creates even greater challenges for the child in the later years when their sensitive information remains permanently online.¹¹¹ The inappropriate and sensitive content could also contribute to problems for the child, such as future humiliation, impersonation, cyberbullying and inappropriate use of the child’s content by paedophiles and sex predators.¹¹² Parents do not always have control over the information that they share although they endeavour to keep the context within selected spheres. The content may inadvertently transcend the initially envisioned boundaries.¹¹³

Beyond the basic sharing of children’s personal information for social reasons, there is a commercial dimension. The digital economy has given rise to online working modalities including the emergency of influencers on social media platforms. Children feature substantially on their parents’ platforms who are influencers. The use of children’s information for developing social media content also exacerbates oversharing of children’s personal information, as previously highlighted. The oversharing is perceived as exploitative and could potentially expose children to online harms such as cyberbullying and unsolicited attention by online predators.¹¹⁴ Social media accounts created by parents on behalf of children are proving to be a conduit for exposing children’s privacy, particularly in situations where they lack the capacity to provide informed consent or object to the dissemination of their images. The UK’s Digital, Culture, Media and Sport Committee published a report on the harms encountered by children assuming roles as influencers on social media platforms.¹¹⁵ The report underscores:

Posting content about children online can affect their privacy, which brings security risks. For example, checking-in to venues on social media posts or posting images of the child’s home could expose their location. Some child influencers, like child stars, have amassed a significant fan base, which could

111 Humanium (n 72).

112 Kopecky and others (n 104) 5.

113 As above.

114 See Sarah Adam’s TikTok account (@mom.uncharted), in which she interrogates the role of parents in creating a digital footprint for their children by posting their personal information over which they do not have control, https://www.tiktok.com/@mom.uncharted/video/7062434975810931974?is_from_webapp=1&sender_device=pc&web_id=6891301529808209413 (accessed 4 July 2022).

115 UK Parliament ‘Influencer culture: Lights, camera, inaction?’ (9 May 2022), <https://publications.parliament.uk/pa/cm5802/cmsselect/cmcumeds/258/report.html#heading-4> (accessed 30 June 2022).

expose them to additional attention when they travel or run fan meet-and-greets.¹¹⁶

Although this is a UK-focused report, it is imperative to recognise that the concerns elucidated are equally pertinent in the African context.

The subject of consent in processing personal information is paramount, but is a complex terrain, generally, and more complicated in the context of children's rights. In the case of a child, it 'neither necessarily expresses a child's autonomy nor protects it, particularly where power imbalances exist'.¹¹⁷ Simultaneously, parental consent may not invariably be the appropriate option as it may not represent the best interests of the child. According to UN General Comment 25 on children's rights in relation to the digital environment, consent should be informed and freely given by either the child or the parent or caregiver. The age and evolving capacity of a child determines the appropriate consenting party prior to processing of data. Data controllers or processors should ensure and validate the acquisition of informed and meaningful consent.¹¹⁸ In Africa, data protection laws mandate the consent of the responsible adult for processing children's personal information, a stance echoed in the legislation of South Africa, Ghana, and Zimbabwe. However, the practical application faces challenges due to the inherent complexities that characterise this domain.

4 Children's actions that compromise their privacy

4.1 Children as online content creators and sharing of personal information

Children actively shape their digital identity and leave a lasting footprint through content creation and dissemination on digital platforms, thereby unconsciously compromising their privacy. The dichotomy between public and private is distorted in the context of the screen-driven culture, compelling children to share content that would otherwise be considered intimate and private, and not intended for public consumption. The propensity to share content online has evolved into a global phenomenon

116 As above.

117 Human Rights Council Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci 'Artificial intelligence and privacy, and children's privacy' (July 2021) para 120, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement> (accessed 31 March 2022).

118 General Comment 25 para 71.

among the young demographics.¹¹⁹ Parents may not be aware of the nature and extent of content creation and dissemination by their children, particularly adolescents. Teenagers perceive online platforms as safe spaces for sharing personal information, including about their dating life.¹²⁰ The South African case presents a quintessential illustration of children overly disclosing intimate personal information. Teenagers as young as 14 years, actively participated under the hashtag #TheRiskITook, which gained popularity on TikTok and other social media platforms. They shared information about reckless sexual conduct that resulted in pregnancy at a young age.¹²¹ The testimonies include images of themselves and their babies. While the hashtag raised awareness on teenage pregnancy it also had privacy implications. They are driven by peer pressure and suboptimal digital hygiene practices reflective of inadequate levels of digital literacy.

For instance, adolescents in South Africa actively participate in the dissemination of sexually explicit material, engaging with both their romantic partners and strangers whom they encounter and form relationships with online.¹²² While the sharing of content occurs with an expectation of privacy, the originator inadvertently relinquishes control over the recipient's subsequent actions with the shared information. Regrettably, instances have arisen where intimate images are disseminated without consent or manipulated into explicit content when relationships turn adversarial.¹²³ The enduring online footprint of these occurrences has the potential to detrimentally impact individuals' reputations, both during their formative years and later in adulthood.

The digitised world is creating new manifestations of child labour where children participate in the digital economy, and assume social media roles as influencers, including on YouTube, Instagram TikTok and generate income for both themselves and their families. They are commonly referred to as 'child influencers' and their cultural currency hinges on popularity which is determined by continuously churning out content to captivate audiences. However, it is within the realm of content creation that the privacy of these children becomes compromised, as they divulge

119 J Orlando 'Online and out there: How children view privacy differently from adults' *The Conversation* (14 April 2015), <https://theconversation.com/online-and-out-there-how-children-view-privacy-differently-from-adults-38535> (accessed 26 June 2022).

120 MacAfee (n 73).

121 LMMM Rantao '#TheRiskITook on sex and pregnancy: Where do we draw the line?' (12 June 2022) *IOL*, <https://www.iol.co.za/sundayindependent/news/africa/theriskitook-on-sex-and-pregnancy-where-do-we-draw-the-line-73879ded-3c6d-4182-922d-0c666bc4568a> (accessed 26 June 2022).

122 Bush (n 58).

123 As above.

sensitive information, including location details and other personal data. This is exemplified in the South African context, particularly observed in children's behaviour in photo-sharing applications and related platforms.¹²⁴

4.2 Sharing of passwords

Younger children, typically characterised by a propensity to share possessions and establish minimal boundaries, exhibit a parallel behaviour in the digital world. Among the various privacy-infringing behaviours observed in children, the act of sharing passwords with friends or romantic partners stands out prominently. This conduct is primarily rooted in trust among friends or signifies the intimacy within a romantic relationship.¹²⁵ However, such sharing compromises the inherent secrecy of a password, a crucial element that preserves the exclusivity of online accounts and acts as a deterrent against unauthorised access. The act of sharing passwords blurs the line between the legitimate account owner and other users with access to the password, potentially distorting the child's unique digital identity.¹²⁶ The termination of friendships or romantic liaisons further exposes password owners, rendering them susceptible and vulnerable.

Besides the imprudent practice with passwords, parents also exercise some degree over a child's digital life by retaining access to their passwords. While it is justifiable for the parents to exercise some degree of control, children should be given the 'freedom to control their own passwords', thereby fostering a deeper understanding of concepts related to privacy and identity, empowering children to navigate the digital landscape responsibly.¹²⁷

4.3 Children Strategies to circumvent parental oversight

In light of their status as digital natives, most adolescents exhibit an advanced technological proficiency surpassing that of their parents and guardians. Leveraging this knowledge, they employ privacy-enhancing measures, denoted as 'monitoring escape action' by Vallejo and others, to

124 'Teens are flocking to new photo-sharing apps. Are they safe?' (22 May 2022) *IOL*, <https://www.iol.co.za/lifestyle/family/parenting/teens-are-flocking-to-new-photo-sharing-apps-are-they-safe-07cb76f5-f8e3-41fd-9864-e2ecd88f48ce> (accessed 26 June 2022).

125 Pew Research Centre: A Lenhart and others 'Teens, kindness and cruelty on social network sites' (9 November 2011), <https://www.pewresearch.org/internet/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/> (accessed 26 June 2022).

126 Popa (n 97).

127 As above.

counteract parental surveillance.¹²⁸ These measures include the strategic selection of applications perceived as ‘safe’ from parental scrutiny, the activation of privacy settings and messaging controls designed to restrict parental access to online activities, and a discerning approach to friend selection that typically excludes parents or guardians.¹²⁹ They may also resort to creation and dissemination of content on platforms unknown to their parental figures and configure profiles as private, limiting access exclusively to friends. The activation of privacy settings allows for the discreet concealment of profile information, activities, likes, and interests, albeit with certain basic details such as name, profile image, and gender potentially remaining accessible by default.¹³⁰ It is also common for pre-adolescents to employ stratagems such as falsifying their ages to gain access to social media platforms that impose age restrictions exceeding their actual age, such as Facebook, Instagram, Pinterest, and X (formerly Twitter).

Notwithstanding the privacy measures implemented to circumvent parental scrutiny, these efforts do not constitute a foolproof shield against potential exploitation. While children may skillfully navigate away from parental scrutiny, their actions position them in situations inherently fraught with the risk of exposure to abuse in the course of online interactions, particularly with strangers harbouring malicious intentions, such as sexual predators targeting teenagers and young adults.

5 Emerging technologies and processing of children’s personal information

The advent of emerging technologies, particularly AI, has become a cornerstone of the 4IR, exerting a profound influence on individuals’ lives, notably those of children. This transformative impact is evident in the digitisation of children’s toys, which are integrated with digital assistants like Alexa and Google Voice.¹³¹ Consequently, emotional and cognitive expressions of children may permeate the structures of toy manufacturing businesses.¹³² AI’s influence is evident in its potential to combat violence against children, particularly in tracking down predators.¹³³ However,

128 Vallejo and others (n 20) 1197.

129 Lenhart and others (n 125).

130 As above.

131 S Steinberg ‘Ethical AI? Children’s rights and autonomy in digital spaces’ (28 April 2021), <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/04/28/children-and-ai/> (accessed 28 March 2022).

132 UNICEF (n 30) 32.

133 Steinberg (n 132).

the use of AI presents ethical concerns, as its deployment may have adverse implications for children's rights, with a particular focus on privacy considerations. The advent of big data similarly yields a dual impact, in that it expedites seamless data retrieval yet concurrently gives rise to substantial privacy concerns. This is especially pronounced when the ethical management of extensive datasets is either disregarded or mishandled.¹³⁴ Additional considerations involve the adept management of sensitive data, particularly health information, and the crucial subject of informed consent. However, despite the growing interest in the intersection of AI and children, the efficacy of this strategic focus is compromised by the inadequate emphasis and scholarly attention directed towards this burgeoning discourse.¹³⁵

6 Existing frameworks in Africa for children's privacy and child protection online

Given the identified risks that children encounter in the digital sphere and the associated privacy challenges, it is imperative to examine the framework designed to safeguard children online, including their privacy. This section highlights the international framework as provided by the UN and the regional and sub-regional framework in the African context. While this framework fundamentally ensures the protection of children's rights, it should be acknowledged that the initial instruments were not designed with the digital environment in consideration. Consequently, treaty-monitoring bodies are presently engaged in formulating standards to address the protection and advancement of children's rights in the digital age. Instruments under consideration are the UN CRC; the African Children's Charter, the African Union Convention on Cyber Security and Personal Data Protection (the (Malabo Convention)); the UN General Comment 25; and General Comment 7 and its Resolution on the Promotion of Children's Rights in the Digital Sphere of the African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee).

6.1 International and regional framework

6.1.1 United Nations Convention on the Rights of the Child

The UN CRC is the international child rights instrument. Adopted in 1989, it contains provisions on the protection of children against various forms of human rights violations. Regarding privacy, article 16 stipulates

¹³⁴ As above..

¹³⁵ As above.

that a child's privacy should not be subject to unlawful and arbitrary infringements, emphasising the need to safeguard their right to privacy through legal means.¹³⁶

6.1.2 UN General Comment 25 on children's Rights in relation to the digital environment

This General Comment, adopted by the Committee on the Rights of the Child in 2021, is specifically tailored to address the promotion and safeguarding of children's rights within the digital context. The Committee recognises that 'innovations in digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the internet'. Based on this position, the Committee sought to guide states on the application of CRC to the digital environment, urging them to enact legislative and other measures. It emphasises the need to respect the perspectives of children; prevention of discrimination; upholding the right to life; ensuring survival and development; and acknowledging the evolving capacities of the child; and prioritising their best interests.¹³⁷

6.1.3 African Charter on the Rights and Welfare of the Child

The African Charter on the Rights and Welfare of the Child (African Children's Charter) is the continental instrument on the rights of the child.¹³⁸ The Charter imposes binding obligations on states concerning the safeguarding of children. Specifically, section 10 underscores the imperative to safeguard the right to privacy. It stipulates that:

No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.¹³⁹

136 Art 16: '(1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. (2) The child has the right to the protection of the law against such interference or attacks.'

137 UN General Comment 25 generally.

138 African Charter on the Rights and Welfare of the Child, <https://au.int/en/treaties/african-charter-rights-and-welfare-child> (accessed 5 March 2022). It was adopted in 1990 and came into force in 1999 (African Children's Charter).

139 Sec 10 African Children's Charter.

6.1.4 *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*

Adopted in 2014, the AU Convention establishes a framework for addressing cyber security, the prevention of cybercrimes, and the safeguarding of personal data. Notably, the Convention incorporates specific provisions on child protection. In this regard, article 29(3) focuses on content-related offences, imposing a legal obligation on member states to criminalise activities related to child pornography, including its production, distribution, registration, transmission, importation, and possession.¹⁴⁰

6.1.5 *African Children's Committee General Comment 7 on article 27 of the African Charter on the Rights and Welfare of the Child on Sexual Exploitation*¹⁴¹

The General Comment expounds on article 27 of the African Children's Charter, specifically addressing the multifaceted issue of child sexual exploitation and abuse.¹⁴² It extensively covers child sexual exploitation online and presents an opportunity to extend the understanding of the implications of article 27 of the African Children's Charter to the digital world of exploitation and abuse.¹⁴³

6.1.6 *Resolution on the promotion of children's rights in the digital sphere*

The Resolution was also adopted by the African Children's Committee in recognition of the negative encounters that children experience in the digital environment.¹⁴⁴ The Committee recognised the need to protect

140 African Union Convention on Cyber Security and Personal Data Protection, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (accessed 5 March 2022).

141 African Children's Committee General Comment 7 on art 27 of the African Charter on the Rights and Welfare of the Child on Sexual Exploitation (2021), https://www.acerwc.africa/wp-content/uploads/2021/09/General-Comment-on-Article-27-of-the-ACRWC_English-1.pdf (accessed 5 March 2022).

142 Art 27 provides: '1. States Parties to the present Charter shall undertake to protect the child from all forms of sexual exploitation and sexual abuse and shall in particular take measures to prevent (a) the inducement, coercion or encouragement of a child to engage in any sexual activity; (b) the use of children in prostitution or other sexual practices; (c) the use of children in pornographic activities, performances and materials.'

143 African Children's Committee General Comment 7 para 10.

144 African Children's Committee Resolution on the Promotion of Children's Rights in the Digital Sphere, <https://drive.google.com/file/d/1WhBF7HGfvyTyxWJmkGsHuavnJhZMrDdd/view> (accessed 5 March 2022).

and promote children's rights to privacy as provided under the African Children's Charter and other instruments such as the Malabo Convention.

6.2 National frameworks

Drawing from the regional and international frameworks, states have an obligation to adopt measures for the lawful processing of personal information including that of children. States are mandated to design regulations for children that are suited for the digital environment, taking into consideration the best interests of the child principle, child protection and privacy as primary considerations. Infringements into children's rights should only be for legitimate reasons and prescribed by the law. Currently, over 30 African countries have adopted specific data protection laws while others have taken a sectoral approach. This section highlights the South African and Rwandan contexts on the protection of children's information and the promotion of digital literacy.

6.2.1 *Protection of Personal Information Act*

South Africa's Protection of Personal Information Act (POPIA) serves as the framework for regulating the processing of personal information including children's personal information. Section 34 prohibits the processing of children's personal information and mandates responsible parties processing children's information apply for authorisation from the Information Regulator. Upon meeting the requisite criteria, additional conditions are imposed to ensure compliance.¹⁴⁵ The Act also mandates that the processing of a child's personal information should be undertaken with explicit consent of a competent person. Such processing should be deemed a requisite measure for defending or exercising a right, or fulfilling a legal obligation.

Furthermore, processing may be permissible for research, statistical, or historical purposes, provided it serves a public interest. It is imperative that adequate safeguards be implemented to ensure the child's privacy, even in situations where obtaining the required consent is unattainable.¹⁴⁶ A child's personal information may also be processed if it is already consciously in the public domain, with the consent of a competent person. The processing may be authorised if the responsible authority has established adequate safeguards for the protection of children and that there exists a compelling public interest justification for the processing. In terms of the law, an individual with competence may withdraw content or

145 Sec 35 POPIA.

146 As above.

seek a review of a child's personal information. Responsible parties may be required to provide notification detailing their processing practices, the amount of information being processed and the nature of children's information that is being processed.

To provide further clarity and guidance on the processing of children's personal information, the Information Regulator, the oversight body with the mandate to oversee the implementation of POPIA, developed a guidance note specifically addressing the processing of children's personal information.¹⁴⁷ It primarily provides guidance to responsible parties who require authorisation to process children's personal information as stipulated in the Act. The guidance note elaborates on appropriate safeguards and public interest. The determination of public interest varies across jurisdictions and requires case-specific assessment given that it is broad and nuanced. It signifies that an undertaking typically yields widespread benefits to the public at large and is essential for fostering justice and equality.¹⁴⁸ In the guidance note the conception of appropriate safeguards is embedded in section 19(1) of POPIA that places a responsibility on the parties processing personal information to ensure its confidentiality and integrity through utilisation of organisational or technical measures to avoid unauthorised access, damage or loss.¹⁴⁹ It is also necessary to establish a comprehensive framework for conducting risk assessment, managing risks and updating existing safeguards, assessing the implementation of the adopted safeguards, taking into account generally-accepted measures and sector-specific safeguards.

6.2.2 *The case of Rwanda's digital ambassadors programme*

In Rwanda, concerted interventions are being undertaken to address the need for digital literacy. A notable initiative is the Digital Ambassadors Programme, a government-funded initiative strategically designed to provide digital literacy to communities.¹⁵⁰ It is a component of the Smart

147 South Africa Information Regulator 'Guidance note on processing of personal information of children' (2021), <https://infoeregulator.org.za/wp-content/uploads/2020/07/GuidanceNote-Processing-PersonalInformation-Children-20210628-1.pdf> (accessed 14 June 2022).

148 As above. Public interest examples in terms of sec 37 of the POPIA include: (a) the interests of national security; (b) the prevention, detection and prosecution of offences; (c) important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); (e) historical, statistical or research activity; or (f) the special importance of the interest in freedom of expression.

149 South Africa Information Regulator (n 148).

150 Government of Rwanda Digital Ambassadors Programme, <https://www.minict.gov.rw/projects/digital-ambassadors-programme> (accessed 16 June 2022).

Rwanda Master Plan.¹⁵¹ Significantly, training sessions are conducted in local languages, with due consideration given to contextual nuances unique to Rwanda. The overarching goal of this initiative is to empower communities to fully harness the potential of digital technologies. This educational intervention serves as a means to ensure that a broad spectrum of community members, encompassing parents and caregivers, are sufficiently proficient in digital technologies. The acquisition of such skills is instrumental in enhancing their proficiency in parenting in the dynamic landscape of the digital age.

The foregoing discussion underscores the inherent risks associated with the digital environment, rendering it unsafe for children to navigate autonomously with absolute privacy. While countries like South Africa and Rwanda have adopted progressive measures in regulating the processing of children's information and promoting digital literacy, these initiatives fall short in addressing the complexities arising from children's online presence and digital technology usage. Comprehensive and nuanced approaches are required in addressing an array of concerns across diverse sectors. The proactive measures undertaken in South Africa and Rwanda are not common practice in Africa. The regulatory framework for the processing of children's personal information is still developing.

7 Lessons for Africa

In the European and US context, technology advancements and integration predate that of Africa and the regulatory frameworks, particularly concerning child online protection, are more mature. This segment of the chapter highlights child protection and privacy measures that African states could consider in fostering healthy digital lifestyles for children. The insights are predominantly derived from advanced European frameworks that extensively address privacy and child protection in the digital sphere. Given the expansive nature of these initiatives, a comprehensive assessment is beyond the scope of this chapter; therefore, only a select few will be explicated for illustrative and lesson-drawing purposes. Selected examples cover general regulations for the protection of children online, data protection in educational settings, guidance for parents, mechanisms

151 Government of Rwanda Smart Rwanda Master Plan (2020), https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/SMART_RWANDA_MASTERPLAN.pdf (accessed 15 June 2022). The Rwandan plan is also inspired by the Smart Africa Manifesto, a 2013 policy document that was adopted by select AU states: Burkina Faso, Gabon, Kenya, Mali, Rwanda, South Sudan, Uganda. It is a statement of commitment 'to provide leadership in accelerating socio-economic development through ICTs'. See <https://smartafrica.org/who-we-are/> (accessed 15 June 2022).

for the protection of children's privacy online, guidelines for digital service providers, and media-specific measures. These examples are presented with the intent that they may be adapted to the African context, and contribute meaningfully to strengthening existing frameworks.

7.1 US Children's Online Privacy Protection Act

The US Children's Online Privacy Protection Act (COPPA) is an example of legislation for children in the digital age. It was in response to the growing use of the internet and introduction of data processing that impacted on children's privacy. It establishes responsibilities for online service providers that serve children below the age of 13. These include notifying parents of information practices, ensuring verifiable parental consent for the processing of children's personal information, affording parents the agency to determine the utilisation of their child's personal information, including the ability to curtail further processing. Additionally, the legislation mandates provision for parental access to their child's personal information, advocates for data minimization by requesting only information that is deemed reasonably necessary, and necessitates the implementation of pertinent procedures to uphold the security, integrity, and confidentiality of children's personal information.¹⁵² In this framework, parents have a basis for controlling personal information that is collected from their children in the digital sphere.

7.2 Guidelines on Children's Data Protection in an Education Setting

Adopted in 2020 by the Council of Europe, these Guidelines are designed to offer guidance to key stakeholders in the education sector, such as policy makers, legislators, data controllers, and the education industry in general, to uphold children's rights in processing children's information. It establishes fundamental principles, including the best interests of the child; the evolving capacities of the child; the right to be heard; and the right to non-discrimination.¹⁵³ It contains specific recommendations directed at legislators and policy makers, data controllers and for the industry.

152 US Government US Children's Online Privacy Protection Act, <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>.

153 Council of Europe 'Children's data protection in an education setting (Guidelines)' (20 November 2020), <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b> (accessed 13 March 2022).

7.3 The UK Children's Commissioner's Guide for Parents

The Guide addresses the manner in which parents ought to engage with their children concerning online sexual harassment, offering essential insights into the ways children navigate the internet and the consequent adverse effects they may encounter. In light of these, it subsequently furnishes parents with counsel on the appropriate methods and timings for addressing these potential pitfalls. It comprehensively explores complex subjects that frequently confront parents, including but not limited to peer pressure, exposure to pornography, the sharing of explicit images (cyberflashing), instances of sexualized bullying, and the manipulation of photographs impacting body image.¹⁵⁴

7.4 UK Code of Practice to protect children's privacy online

Adopted in 2020 under the auspices of the UK Information Commissioner, the age-appropriate design Code of practice for online services sets out 15 standards for the protection of children's privacy.¹⁵⁵ It is targeted at 'those responsible for designing, developing or providing online services like apps, connected toys, social media platforms, online games, educational websites and streaming services'.¹⁵⁶ The core tenet embodied in the Code is the requirement for service providers to set high standards for default privacy settings on services and other digital products that might be accessed by children, taking due consideration of the best interests of the child.

7.5 OECD Recommendations on the Protection of Children Online

The Recommendations were initially adopted in 2012 and amended in 2021, in response to the risks that children encounter in the digital environment.¹⁵⁷ The 2021 amendments took into account advancements

¹⁵⁴ As above.

¹⁵⁵ UK Information Commissioner 'The age appropriate design: A code of practice for online services' (2020), <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/> (accessed 13 March 2022).

¹⁵⁶ UK Information Commissioner 'ICO publishes Code of Practice to protect children's privacy online' (21 January 2020), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/> (accessed 13 March 2022).

¹⁵⁷ OECD Recommendation of the Council on Children in the Digital Environment (2021), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389%20> (accessed 13 March 2022).

in technology and additional risks as a result of the COVID-19 pandemic. The Recommendations recognise the significance of protecting children's data and their privacy for their autonomy and well-being. Consequently, it is essential to empower children so that they 'become confident and competent users of digital technology'.¹⁵⁸ The Recommendations establish principles for a safe and beneficial digital environment for children, encompassing fundamental values; empowerment and resilience; proportionality and respect for human rights; appropriateness and inclusion; and shared responsibility, co-operation, and positive engagement.¹⁵⁹ The Recommendations also include policy-related proposals. These entail the demonstration of leadership and commitment taking into account the best interests of the child in the digital environment;¹⁶⁰ the review, development and amendment of laws that impact on children in the digital environment; the promotion of digital literacy; the adoption of evidence-based policies to support children in the digital space; and the promotion of measures that 'provide for age-appropriate child safety by design'.¹⁶¹ The concluding segment underscores the imperative of international collaboration, with specific reference to the OECD Guidelines for Digital Service Providers, recognised as pivotal in safeguarding children's online welfare.

7.6 OECD Guidelines for Digital Service Providers

The Guidelines were adopted in 2021 and complement the Recommendations on the Protection of Children Online.¹⁶² They are aimed at providing guidance to service providers

when they take actions that may directly or indirectly affect children in the digital environment, in determining how best to protect and respect the rights,

158 As above.

159 As above.

160 These include: (a) adopting clear policy objectives at the highest level of government; (b) articulating a whole-of-government approach, through a national strategy where appropriate, that is flexible, technology neutral, and coherent with other strategies for fostering a sustainable and inclusive digital economy; (c) consider establishing or designating oversight bodies, with a view to: (i) coordinating stakeholders' views, efforts, and activities in the development of policies; (ii) meeting policy objectives; (iii) reviewing the effectiveness of policy actions and measures implemented to account for the best interests of children in the digital environment; (iv) coordinating, in accordance with their legal and institutional frameworks, the relevant actions of government bodies with responsibility for responding to the needs of children; (v) ensuring that the actions of government bodies are cohesive and mutually reinforcing, rather than an accumulation of isolated or stand-alone, and potentially inconsistent, initiatives; and (vi) promoting co-operation across borders.

161 OECD (n 160).

162 As above.

safety, and interests of children, recognising that girls, children belonging to racial, ethnic and religious minorities, children with disabilities, and others belonging to disadvantaged groups may require additional support and protection.¹⁶³

The Guidelines acknowledge the nuances in the nature of service providers and identify three broad specific measures that could be adopted by service providers. These are taking a precautionary approach by adopting the child safety by design option; proactively providing sufficient relevant information in a transparent manner; and informing relevant actors, such as children, parents and any other persons with parental responsibility, all the required information about data processing. Finally, the Guidelines urge service providers to establish governance and accountability mechanisms that promote the best interests of the child when accessing their products and services.¹⁶⁴

7.7 BBC editorial guidelines for safeguarding children's online safety

The editorial guidelines of the British Broadcasting Corporation (BBC) encompass directives regarding the engagement with children and young individuals in online platforms.¹⁶⁵ The BBC provides explicit and comprehensive thematic instructions that pertain to various aspects, including but not limited to issues of privacy;¹⁶⁶ children and young people and content contributors;¹⁶⁷ harm and offence;¹⁶⁸ competitions, votes and interactivity.¹⁶⁹

163 As above.

164 OECD 'Guidelines for digital service providers', <https://legalinstruments.oecd.org/public/doc/272/5803627d-b49b-4894-8dbe-35f67fd10007.pdf> (accessed 13 March 2022).

165 British Broadcasting Corporation 'Guidance: Interacting with children and young people online', <https://www.bbc.com/editorialguidelines/guidance/children-young-people-online#guidanceinfull> (accessed 13 March 2022).

166 BBC 'Guidance: Privacy', <https://www.bbc.com/editorialguidelines/guidelines/privacy/> (accessed 13 March 2022).

167 BBC 'Guidance: Working with children and young people as contributors', <https://www.bbc.com/editorialguidelines/guidance/children-young-people-working/> (accessed 12 March 2022).

168 BBC 'Editorial guidance: Harm and offence', <https://www.bbc.com/editorialguidelines/guidelines/harm-and-offence/> (accessed 12 March 2022).

169 BBC 'Editorial guidance: Competitions, votes and interactivity', <https://www.bbc.com/editorialguidelines/guidelines/competitions-votes-interactivity/> (accessed 12 March 2022).

7.8 UNICEF Guidelines for Industry on Child Online Protection

Adopted in 2015, the UNICEF Guidelines are designed to protect child safety online.¹⁷⁰ They target governments, schools and industry. Broadly, the Guidelines

- (a) establish a common reference point and guidance to the ICT and online industries and relevant stakeholders;
- (b) provide guidance to companies on identifying, preventing and mitigating any adverse impacts of their products and services on children's rights;
- (c) provide guidance to companies on identifying ways in which they can promote children's rights and responsible digital citizenship among children;
- (d) suggest common principles to form the basis of national or regional commitments across all related industries, while recognising that different types of businesses will use diverse implementation models.¹⁷¹

The Guidelines contain a sector-specific checklist addressing various facets of promoting digital technology for civic engagement; digital literacy for parents, teachers and children; and the creation of age-appropriate online content. Additionally, the Guidelines advocate for the establishment of standardised procedures for managing child sexual abuse material and the integration of children's rights into corporate and management policies.¹⁷² The specific sectors covered by these Guidelines are broadcasting services, mobile operators, internet service providers; media service providers, application stores, hardware developers and operating systems developers.

The selected examples from Europe and the US serve as valuable benchmarks for the development of region-specific strategies in Africa aimed at ensuring children's online protection and safeguarding their privacy. The detailed recommendations delineating these strategies are outlined in the subsequent part of this chapter.

8 Conclusion and key recommendations

The examination of child online risks and their privacy implications underscores the imperative for states to implement appropriate measures.

170 UNICEF 'Guidelines for industry on child online protection' (2015), <https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf> (accessed 16 June 2022).

171 As above.

172 As above.

The ensuing recommendations are directed towards policymakers, the business sector, the media, schools, and other pertinent institutions tasked with managing children's information. A default adherence to high standards of child privacy should be instituted for platforms and digital devices catering to children, accompanied by the provision of mechanisms for redress in cases of privacy breaches. Embracing preventive measures, robust safeguards, and restorative justice in all its forms should constitute the foundational approach to online child protection and privacy.¹⁷³ While incorporating privacy-enhancing technologies, such as encryption, it is essential to ensure they do not impede the detection and reporting of child-based exploitation online. Also, upholding the principles of legality, necessity, and proportionality is paramount.¹⁷⁴ These recommendations draw heavily from the insights outlined in UN General Comment 25 as well as research findings from UNICEF.

8.1 States

In the wake of a global transformation ushered in by digitisation, the state remains the duty bearer as the primary protector and assumes the role of providing the overarching guidance on online child protection and privacy through legislative and other measures. The UN General Comment 25 underscores the imperative for states to enact measures ensuring the protection of children in the online sphere. In order to harmonise and advocate for diverse perspectives and requirements of children based on various variables, all policy advancements should align with international human rights and standards, incorporating consultations with children and institutions dedicated to promoting children's rights and welfare.¹⁷⁵ The recommendations for the state that will be discussed focus on legislative and policy measures for child protection and privacy and data protection; the education sector; parents and caregivers; the media and civil society; and public and private sector institutions. The state's obligations concerning child protection emanate from the CRC, the Africa Children's Charter, soft law instruments that have been developed by the UN Committee on the Rights of the Child and the African Children's Committee; and other relevant international and regional instruments such as model laws, conventions and guidelines.

173 General Comment 25 para 81.

174 General Comment 25 para 70. Any decision to decrypt children's data for criminal investigation on online crimes that are perpetrated against children, such as child sexual abuse and exploitation, should be proportionate and in the best interests of the child. See also UNICEF (n 30) 32.

175 UNICEF (n 30) 35.

8.1.1 *Child safety and privacy and data protection frameworks*

Ensuring the efficacy of children's rights legislation and policies requires regular scrutiny to ascertain their compatibility with the evolving digital landscape and alignment with the best interests of the child. This entails the enactment of laws and policies designed to shield children in the online sphere, safeguarding the confidentiality and integrity of their personal information.¹⁷⁶ Amendments to existing legislation conceived without foresight into the digital age are necessary, alongside the introduction of new laws tailored to address contemporary challenges. Concurrently, the establishment of relevant institutions is vital to oversee and enforce these regulations. Noteworthy is the UK's establishment of a children's commissioner dedicated to addressing online protection concerns. Conversely, the challenge in Africa lies in the implementation of existing frameworks. To rectify this, a more robust sectorial or thematic approach is recommended, facilitating the formulation of additional regulations or guidance relevant to the protection of children's rights in the digital realm.

8.1.2 *Recommendations for digital literacy*

States should ensure that, in the implementation of measures aimed at realising the right to education, education policies explicitly incorporate media and digital literacy, seamlessly integrating them into both school and teacher training curricula.¹⁷⁷ Recognising digital literacy as a fundamental life skill is paramount, serving as a critical mechanism for effectively navigating the complexities of the digital world, including its inherent risks.¹⁷⁸ The inclusion of digital proficiency skills within teacher training

176 General Comment 25 para 70. The fundamental point is that children's personal information should not be arbitrarily accessible except by designated entities, for specified duration and purposes in line with the law. See General Comment 25 para 73.

177 UNESCO Policy Brief: Digital Literacy in Education 7, https://iite.unesco.org/files/policy_briefs/pdf/en/digital_literacy.pdf (accessed 16 June 2022). See also Berson & Berson (n 6) 142. Berson and Berson conceptualise digital literacy as 'a compilation of legal precedent, voluntary policies, and ethical conduct. It represents the ability to access digital forms of information, critically evaluate its quality and utility, analyse information for connections to and expansions of knowledge, and use digital tools to produce original works. It emphasises the capacity to fully participate as a responsible member of a technologically engaged society and refers to the skills that people need to understand and constructively navigate the digital media that surrounds them. It addresses safety and security while fostering broader preparation for digitised and networked environments.'

178 Berson & Berson (n 6) 142-143. See also Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 118. In his report Cannataci also affirmed that '[d]igital literacy education can prevent harmful online behaviour at its source', so 'children and adolescents need operational skills and cognitive and social abilities to use technologies in thoughtful, ethical and safe ways'. This should be in addition to the

programs empowers educators to adeptly guide learners on crucial aspects of the digital environment, such as safety and privacy. Within African communities facing challenges associated with the digital space and technological innovations, parents and caregivers often find themselves insufficiently prepared to navigate the complexities of parenting in the digital age. Notably absent are targeted programs addressing the unique needs of parents and caregivers. Consequently, states should proactively adopt policy measures that foster opportunities for parental digital literacy, equipping parents with the necessary tools to safeguard their children, particularly the younger ones, in the digital environment.¹⁷⁹ These tools include managing online relationships, ensuring the secure sharing of personal information, reporting abuse, implementing effective filtering, age verification, and password protection – all pivotal components contributing to online safety.¹⁸⁰ An example of community digital literacy is the previously-discussed Rwandan Digital Ambassadors Programme.

However, controversies surround the efficacy of digital literacy as a comprehensive strategy for mitigating digital risks. Despite efforts to impart knowledge to children, educators, and parents about the intricacies of the digital landscape and its implications for safety and privacy, the inherent challenge is multifaceted. In tandem with fostering digital literacy, a recalibration of the conditions governing data processing is necessary, with a primary emphasis on the responsibilities of service providers.¹⁸¹ Scrutiny of prevailing data processing conditions reveals a lack of clarity, thereby complicating the ability of children and parents to navigate the system effectively. The underlying reality is that, on occasion, these conditions are not optimised to facilitate the seamless management of one's data.¹⁸²

8.1.3 Recommendations for schools and other educational institutions

The digitisation of the education sector significantly impacts the processing of children's data. Educational institutions process information such as class videos, academic performance, attendance, age, address, sex

privacy engineering of digital technologies that technology companies should adopt. See para 123.

179 General Comment 25 para 21.

180 UNICEF (n 30) 34.

181 S Livingstone “‘It’s none of their business!’ Children’s understanding of privacy in the platform society’ (15 August 2020), <https://blogs.lse.ac.uk/parenting4digitalfuture/2020/07/15/privacy-in-the-platform-society/> (accessed 9 March 2022).

182 As above.

and ethnicity. Additionally, some schools install surveillance cameras in classrooms or school premises. Given the mandatory nature of education, some of the regulations associated with it are seldom contested by learners or parents, potentially leading to a lack of scrutiny. In the absence of robust safeguards, regulations, and security measures, there exists a risk of data collection that falls outside the boundaries defined by data protection principles. These principles include, but are not limited to, obtaining meaningful consent, practising data minimization, ensuring accountability, minimising the purpose of data usage, maintaining transparency, and ensuring data accuracy.¹⁸³ The onset of the COVID-19 pandemic and the subsequent shift towards virtual education underscored a prevalent disregard for child data privacy laws, notwithstanding the extensive digital footprints generated by virtual learning, thereby heightening privacy concerns.¹⁸⁴ While the processing of a child's information in the education sector serves legitimate purposes, it is imperative that such processing adheres strictly to established data protection principles.¹⁸⁵

The education sector manages substantial volumes of children's information, thereby creating potential avenues for abuse in the absence of strict regulatory adherence. A notable concern involves the unlawful and unauthorised utilisation of students' accounts, facilitating access to inappropriate content and enabling engagement in illicit activities, thereby posing a significant risk of long-term reputational harm to the child.¹⁸⁶ Such situations emanate from weak password management systems, particularly when custodianship of passwords is vested in administrators. Addressing these irregularities and vulnerabilities is crucial to safeguarding the integrity and security of students' information in the education sector.¹⁸⁷

8.1.4 Recommendations for private institutions

According to Third and others, 'it is timely and important to assert states' obligations to ensure that businesses bear their responsibilities regarding children's rights.'¹⁸⁸ In this regard, states should adopt policies that govern the processing and management of data by both public and private entities,

183 Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 107.

184 As above.

185 General Comment 25 para 73.

186 Popa (n 97).

187 As above.

188 Third and others (n 2) 387.

with a primary focus on safeguarding children's data.¹⁸⁹ The legal and policy framework should expressly mandate that any institution engaged in the processing of children's data formulates and implements robust child protection policies, specifically tailored to address online threats and prevent various forms of abuse such as the exploitation of children's information for commercial benefits. This encompasses mitigating the exploitation of children's information for commercial gains, exemplified by the monetization of such data for targeted marketing and advertising purposes. This could through the establishment and enforcement of child-specific ethical standards, integrating paramount considerations of privacy and security measures into the broader framework.¹⁹⁰

The UN Guiding Principles on Business and Human Rights provides a framework from which states should regulate the conduct of businesses in the spectrum of human rights.¹⁹¹ Central to this framework is the foundational principle that 'states must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises'.¹⁹² Businesses, on the other hand, bear the responsibility to uphold and 'respect human rights throughout their operations'.¹⁹³ Complementary to these principles, UNICEF also developed guidelines for industry on child online protection.¹⁹⁴ Service providers, particularly social media platforms, bear the responsibility of ensuring that their terms and conditions, privacy policies, and data protection policies are presented in a manner that is easily comprehensible and accessible to both children and parents. In fulfilling their duty-bearing role, states must establish an enabling environment conducive to the realisation of these objectives. This necessitates the implementation of relevant legislative and policy frameworks by the state to regulate the conduct of businesses in alignment with the outlined principles.

The legislative framework should comprehensively address the multifaceted responsibilities of business enterprises including implementation; enforcement mechanisms; and mechanisms for redress.

189 Third and others (n 2) 387.

190 UNICEF (n 30) 34.

191 United Nations 'Guiding principles on business and human rights', https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed 9 March 2022).

192 As above.

193 As above.

194 UNICEF 'Guidelines for industry on child online protection' (2015), <https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf> (accessed 16 June 2022).

The responsibilities entail imposing obligations for businesses to design their platforms in a manner that serves the best interests of the child.¹⁹⁵ The legislation should also mandate businesses to report online exploitation and abuse of children to law enforcement or other designated authorities.¹⁹⁶ A critical component of the regulatory framework should involve the establishment of a robust sanctions regime specifically tailored for offences related to online child exploitation. Clear and accessible mechanisms for redress must be articulated within the legislative framework.

As elucidated earlier, the diverse range of harms experienced by children online necessitates that social media platforms refrain from disseminating child abuse content. These platforms should proactively establish deterrent mechanisms against offenders utilising their platforms for the collection and distribution of information resulting in child abuse and exploitation. Collaborative efforts with law enforcement agencies and other pertinent entities are imperative to effectively combat online criminal activities targeting children.¹⁹⁷

Another important recommendation pertaining to both private and business entities involves conducting children's rights impact assessments (CRIAs) and child rights impact evaluation (CRIE). CRIA, an evaluative process undertaken prior to the implementation of any action or decision, serves to ascertain the potential impact of proposed measures on children. Conversely, CRIE systematically examines both the intended and unintended consequences of decisions or actions on the rights of children. Undertaking these assessments guarantees a holistic approach that is thorough and inclusive, encompassing the entirety of children's rights.¹⁹⁸ Therefore the imperative of governmental bodies, civil society, and regulatory authorities to hold businesses accountable in this regard cannot be overstated.

8.1.5 Recommendations for the media and civil society

The media is a significant stakeholder in online child protection and their privacy. Its influence extends to fostering or perpetuating the vulnerability

195 Livingstone (n 186).

196 UNICEF 'Legislating for the digital age', <https://www.unicef.org/media/121261/file/Legislating%20for%20the%20digital%20age%20.pdf> (accessed 20 May 2022).

197 UNICEF (n 30) 34.

198 E Lievens and others 'The child right to protection against economic exploitation in the digital world' (2019) 4, <https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/OtherStakeholders/EvaLievensSimonevanderHofetal.pdf> (accessed 9 March 2022). This is a submission during the drafting of General Comment 25.

of children in the digital sphere. The media as an evolving sector is also using technology innovations that have an impact on children. Particularly when children are contributors of online content, it becomes imperative to observe due considerations for their privacy and secure parental consent. To uphold ethical standards and ensure diligence, media outlets should engage child experts in scrutinising children's content prior to publication. Upholding high ethical standards and exercising due diligence should be integral to all media engagements involving children.

In its approach to children in the digital age, states should actively collaborate with civil society organisations. Child-led groups and child-rights advocates and other organisations with a focus on digital rights are important allies in the implementation of initiatives related to the promotion and protection of children's rights in the digital environment.¹⁹⁹ Both the media and civil society bear a shared responsibility in strengthening public awareness and fostering digital literacy. Advocates for digital rights should conceptualise interventions aimed at equipping children and communities with essential digital skills. Illustrating the media's role, the Share Aware campaign in the United Kingdom, spearheaded by the National Society for the Prevention of Cruelty to Children, serves as an exemplary initiative. This media campaign is purposefully designed to impart knowledge to children about cyber safety and underscore the significance of safeguarding their personal information.²⁰⁰

9 Conclusion

The initial design of the digital landscape did not prioritise children but their presence has escalated in this domain. It is therefore imperative to continuously establish protective mechanisms in this dynamic evolving digital landscape, to minimise their susceptibility, considering that it has become integral to children's lives. This presents opportunities and risks, heightened by the amplified online engagement during the COVID-19 pandemic. While the pandemic response propelled children's access to digital devices and the internet, it is crucial for states, as duty bearers, to regulate the digital environment in a manner that upholds and respects the best interests of every child. The formulation of such interventions requires a multi-stakeholder approach in alignment with international human rights standards. In this regard, it is important to clarify the

199 UN General Comment 25 para 34.

200 J Orlando 'Online and out there: How children view privacy differently from adults' *The Conversation* (14 April 2015), <https://theconversation.com/online-and-out-there-how-children-view-privacy-differently-from-adults-38535> (accessed 31 March 2022).

stakeholder roles in promoting children's privacy and online safety, for the sustained success of interventions.

The imperative to shift perspective from perceiving children solely within the framework of vulnerability is underscored, advocating for their acknowledgment as rights holders. Active inclusion of children in pertinent regulatory and policy dialogues is necessary, accompanied by comprehensive awareness campaigns aimed at navigating technologies for children, parents, caregivers, and educators. Realising this goal necessitates the establishment of collaborative alliances between the state and stakeholders in the education sector, child rights civil society organisations, academia, the media, the private sector, legal professionals, and communities at large.²⁰¹ An overprotective approach unnecessarily limits children's rights to privacy and expression, which should not be limited arbitrarily. Where data protection legislation or other regulatory frameworks are adopted, they should respect child privacy and the protection of their personal information. As children spend more time online and use automated systems, through education, social media interactions or gaming, service providers should adopt the privacy by design approach. They should continuously review their data protection practices and policies and align them with the best interests of the child.²⁰² A rights-based and multi-stakeholder approach should be adopted in integrating the privacy and protection agendas.²⁰³

Robust research, including continuous assessment and evaluation is also crucial in understanding the complexities of children's digital experiences. This recommendation requires a nuanced approach particularly in the context of data collection, which should take into account the various dimensions such as socio-economic background, gender, sex, language, location, ethnicity, age, race and disability. The insights gleaned from such research forms the basis for possible action. Finally, while acknowledging the risks, it is imperative to underscore the significance of privacy in fostering children's psychosocial and autonomous development. The efficacy of the proposed recommendations hinges on the adoption and effective implementation of legislative and other measures by states, striking the delicate balance between the right to privacy and online protection. Regular reviews are also important considering the fast paced

201 Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 30.

202 These approaches should also encompass sports and entertainment premises, educational institutions, business premises, homes, streets and shopping centres. See General Comment 25 para 74.

203 Berson & Berson (n 6) 145. See also Report of the Special Rapporteur on the right to privacy, Joseph A Cannataci (n 117) para 117.

evolution of technology advancements, which also intensifies digital risks for children.

References

- Berson, IR & Berson, MJ 'Children and their digital dossiers: Lessons in privacy rights in the digital age' (2006) 21 *International Journal of Social Education* 136
- Calvoz, RR and others 'Constitutional implications of punishment for cyber bullying' (2014) *Cardozo Law Review*
- Gligorijevic, J 'Children's privacy: The role of parental control and consent' (2019) 19 *Human Rights Law Review* 202
- Kopecky, K and others 'The phenomenon of sharenting and its risks in the online environment: Experiences from Czech and Spain' (2020) 110 *Children and Youth Services Review* 2
- Laubscher, M & van Vollenhoven, WJ 'Cyberbullying: Should schools choose between safety and privacy?' (2015) 18 *Potchefstroom Electronic Law Journal* 2219
- Mathiesen, K 'The internet, children, and privacy: The case against parental monitoring' (2013) 15 *Ethics and Information Technology* 263-264
- Ouvrein, G & Verswijvel, K 'Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management' (2019) 99 *Children and Youth Services Review* 320
- Slonje ,R & Smith, PK 'Cyberbullying: Another main type of bullying?' (2008) 49 *Scandinavian Journal of Psychology* 147-154
- Third A and others 'Recognising children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice' in Wagner B and others (eds) *Research handbook on human rights and technology Global Politics, Law and International Relations* (United Kingdom: Edward Elgar Publishing, 2019)
- Vallejo, MG and others 'Kids and parents privacy exposure in the internet of things: How to protect personal information?' (2018) 22 *Computación y Sistemas* 1196

7

GENDERED DIGITAL INEQUALITIES: HOW DO WE ENSURE GENDER TRANSFORMATIVE LAW AND PRACTICE IN THE AGE OF ARTIFICIAL INTELLIGENCE IN AFRICA?*

Chenai Chair

Abstract

The advent of digital technology in Africa presents a dual narrative, offering both promise and peril as nations strive to integrate into the global digital landscape. While digital advancements hold potential for developmental and economic progress, the continent grapples with stark gender disparities in internet access, with women and gender-diverse individuals disproportionately affected. As governments design strategies to harness digital tools for societal advancement, foreign tech firms flock to support these initiatives, particularly in emerging fields like artificial intelligence (AI) and machine learning. This chapter examines the intricate interplay between AI development and data dynamics, emphasizing the gendered dimensions of privacy and data protection. Through a gender-centric lens, it advocates for inclusive policies within the Southern African Development Community (SADC), notably in South Africa, guided by feminist principles of the internet and data feminism. Drawing on primary research with stakeholders, including activists and legal experts, the chapter underscores the imperative of a nuanced approach to AI governance, one that safeguards against exacerbating existing inequalities while fostering a more equitable digital future. Recommendations for policymakers and civil society underscore the need for proactive measures to ensure that digital innovations uphold, rather than undermine, fundamental rights and societal equity.

1 Introduction

The aspirations of African countries and governments to be connected to the new digital ecosystem presents a double-edged sword on what it means to be part of the digital world. Digital technology is seen as part of the solution to the problems that African countries face from a developmental and economic growth perspective. According to the 2019 International Telecommunication Union (ITU) ICT statistics, over half of the world

* This research was made possible by a research grant from the Mozilla Foundation awarded to the researcher as a Tech Policy Fellow in 2019/2020. The complete research project is available on mydatarights.africa including a South Africa-specific paper. The views expressed are entirely those of the researcher.

is estimated to be connected to the internet. In Africa, only a third of the individuals on the continent use the internet, constituting 37 per cent of the male population as compared to 20 per cent of the female population – indicating a gender digital divide.¹ Women and gender-diverse people already bear the societal brunt of inequality, which extends to the digital space.

African governments are developing strategies and policies to ensure access to and use of digital technology in all spheres of life while foreign-based technology companies are convening on the continent to support the technology roll-out. New emergent technologies, in particular, artificial intelligence (AI) and machine learning-based solutions, have become the focus of digital development in a race to be technologically ready for the Fourth Industrial Revolution (4IR). These technologies are found in daily services as people use social media platforms relying on algorithms for moderation and content direction, and in financial services with automated decision-making systems determining who has access to services. Kenya, South Africa, Tunisia and Nigeria are some of the main digital technology hubs developing ways to support AI-based innovations with a thriving start-up ecosystem. However, the development, implementation and governance of these AI-based innovations in the context of inequality, especially around data fed into them, raises important questions as to their impact on society and digital rights.

This chapter is concerned with the way in which personal and non-personal information feeds into the development of AI-based innovations, and regardless of it being in the form of aggregated data sets, shapes how people experience privacy from a gender and sexual orientation perspective. Focusing on gender inequalities in the conversation demands a gender-centred approach to interrogating new technologies that are being implemented, from conceptualisation and design to the safeguards that have been put in place to ensure that inequalities are not increased or new ones formed.

A gender lens is used to propose ways of ensuring gender-responsive laws and policies to privacy and data protection in the Southern African Development Community (SADC) with an extensive focus on South Africa. Feminist principles of the internet and data feminism are conceptual tools used to conduct research and analyse findings.

1 'Measuring digital development – ITU facts and figures 2019', https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019_r1.pdf (accessed 20 September 2021).

Primary research is conducted with identified digital rights, gender and sexual justice activists, technical community and policy analysts, and legal experts to gauge awareness and concerns regarding privacy and data protection with the uptake of AI-based innovations. The chapter highlights the context to indicate the issues in which these systems are embedded. Considerations of what a gender-responsive law would look like are provided with recommendations for policy makers and civil society.

2 Conceptual framework and approach

The replication of existing inequalities, development of new social injustices and unequal power dynamics impact the difference in experiences of decisions made by algorithms from AI and machine-learning systems. A feminist approach is used to assess the issues at hand beyond compliance for economic engagement, rather the social aspects of using the technology within the context of social inequalities. Context is central to understanding what may be done to address the issues at hand from a gender perspective. The research questions are (i) what a gender-responsive data protection and privacy law would entail to ensure gender transformative law and practice; (ii) how civil society can play a role in ensuring a gender-transformative law and practice with a focus on the right to privacy.

2.1 Feminist conceptualisation

The replication of existing inequalities, the development of new social injustices and unequal power dynamics impact the experiences of these new technologies with significant impacts on marginalised communities. This research is conducted from a gendered perspective and takes on feminist approach in understanding the issues of concern,² drawing from the concepts of data feminism, feminist principles of the internet, intersectionality, and data justice. The novelty of this work in the African region lends itself to drawing from different schools of thought that underpin feminist thought.

The study draws on data feminism principles to guide its methodology.³ The principles are examining power – the way it operates in the world; challenging power – to push back against these power dynamics and work towards justice; rethinking binaries – challenge the gender binary

2 C Chair 'A feminist approach to assessing AI, privacy and data protection in South Africa' (2020), <https://mydatarights.africa/a-feminist-approach-to-assessing-ai-privacy-and-data-protection-in-south-africa/> (accessed 20 September 2020).

3 C D'Ignazio & LF Klein *Data feminism* (2020).

and binaries that lead to oppression; embracing pluralism – bringing together multiple perspectives while prioritising lived experiences of the communities affected and focusing on local and indigenous knowledge; considering context – locate this conversation in context to understand the unequal social relations; make labour visible and elevate emotion; and the embodiment of value in multiple forms of knowledge. These guiding principles allow for critical engagement and centring of society in relation to technology and current laws. In centring society, we focus on its differences, challenging neutral approaches to law and technology. A feminist approach allows one to ask questions of who is being represented and by whom; whose interests are being centred; why this discussion is important and how it is taking place, allowing for criticism of power and how data can be used to ensure justice in society.⁴

The feminist principles of the internet on privacy and data protection also form the underlying conceptualisation of this work. The cluster of agency specifically involves building the politics of consent into the culture, design, policies, and terms of service of internet platforms; the right to exercise and retain control over our personal history and memory on the internet; the right to privacy and total control over personal data and information online; the right to be anonymous; the inclusion of the voices and experiences of young people in the decisions made about safety and security online; and the agency to address and find solutions to the issues of online harassment and technology-related violence.⁵

The experiences of inequality in society are different. In this study, intersectionality allows us to look at the layers of inequalities based on the different spaces we occupy. Crenshaw highlights that intersectionality allows us to see inequality of gender experienced at various points, including race, where you stay, the class you occupy and sexuality.⁶ Furthermore, Hill-Collins shows that there are domains of power in which we exist at different times that shape our experiences of opportunities and inequalities at varying intersectionalities.⁷ Hill-Collins identifies four domains of power: the structural domain – the design and focus of the law; the disciplinary domain – the way things are done; the hegemonic domain – norms that drive the space; and the interpersonal domain – how we relate to one another. The intersectional approach allows for an understanding of gender-responsive laws that consider multiple inequalities and locate

4 As above.

5 <https://feministinternet.org/> (accessed 28 September 2020).

6 K Crenshaw 'Mapping the margins: Intersectionality, identity politics, and violence against women of colour' (1991) 43 *Stanford Law Review* 1243.

7 PH Collins *Intersectionality as critical social theory* (2019) 3.

technology in the context of systematic oppressions, including racism, sexism, colonialism, classism, and patriarchy. As Tamale writes, ‘while Africans are adversely affected by enduring legacies of colonialism and its convergence with racism, our positioning within diverse social categories based on gender, ethnicity, class, sexuality, disability, religion, age, marital status etc. means we experience oppression differently’.⁸

Feminist research is interested in how the work it does contributes to how technology may be used for transformational change in society for women, gender-diverse and vulnerable groups on the basis of class, sexuality or ethnicity.⁹ The research is interested in ensuring data justice as part of the wider underpinnings of a feminist approach. Fraser’s work on abnormal justice challenges us to rethink justice by focusing on ‘what of justice, who of justice and how of justice as a disruptive way of thinking of justice’.¹⁰ A data justice approach acknowledges the complexity of the new technology systems and how they can be used to discriminate, discipline and control; take into account the positive and negative potential of these new technologies and use principles useful across varying contexts.¹¹ The data justice approach privileges social conditions and lived experiences of those who are subject to domination and oppression in society. Our entry point is not the data system itself but rather ‘the dynamics upon which data processes are contingent in terms of their development, implementation, use and impact’.¹²

2.2 Methodology: Qualitative and quantitative

The research, guided by feminist epistemologies, uses a mixed methods approach of quantitative and qualitative data to collect primary data. The complexity of the topic called for a mixed methods approach to understand the issue at hand better allowing for multiple perspectives of knowledge.¹³ Secondary research was also conducted from literature and an assessment of current legislation related to digital rights – specifically

8 S Tamale *Decolonisation and Afro-feminism* (2020) 94.

9 TS Hussen ‘“All that you walk on to get here”’: How to centre feminist ways of knowing’ 2019, <https://genderit.org/editorial/all-you-walk-get-there-how-centre-feminist-ways-knowing> (accessed 28 September 2020).

10 N Fraser ‘Abnormal justice’ (2008) 34 *Critical Inquiry* 398.

11 L Taylor ‘What is data justice? The case for connecting digital rights and freedoms globally’ (2017) 4 *Big Data and Society* 2.

12 L Dencik and others ‘Working paper: A conceptual framework for approaching social justice in the age of datafication’ 2018, <https://datajusticeproject.net/> (accessed 18 June 2020).

13 A Tandon ‘Feminist methodology in technology research: A literature review’ 2018, <https://cis-india.org/internet-governance/> (accessed 28 September 2020).

privacy and data protection. The purpose was to understand the current laws in place to the extent to which they are gender-responsive and develop recommendations from there. A qualitative method of interviews was implemented in which ten individuals from the technical, academic and legal communities working on AI were interviewed who have worked on issues of gender, privacy and data protection globally and with expertise in the SADC region. A quantitative closed-ended targeted survey, drawing from the snowball sampling methodology, was used to engage activists working in the gender and sexual justice community. The survey was a tool to gauge awareness and concerns of the right to privacy and data protection considering AI uptake in South Africa for a specific group of people. In total, 25 participants engaged with the survey, which included open-ended questions. The participants represented multiple workspaces such as research, media, human rights, and sexual reproductive health rights that are ultimately focused on gender inequality issues (see table 1). They work across women and gender diverse communities which allows for an intersectional approach to understanding the issues at hand and multiple forms of knowledge and centring marginalised communities.

Table 1: Survey participants’ areas of work and community engagement

Occupation	Area of engagement
Research	Women and girls, LGBTIQ community, disabled community, sex workers
Media and communications	Women and girls, LGBTIQ community, disabled community, sex workers
Gender and sexuality rights	Women, LGBTIQ community
Research	Women, women and girls, LGBTIQ community
Tech policy and human rights	Digital rights issues
Activism - Academia; research	LGBTIQ community
gender and human rights	Women, working class communities, migrants and undocumented communities
Marketing, branding and communications	Women, LGBTIQ community
Young women’s rights, digital rights	Women and girls, LGBTIQ community, working class communities

Policy and advocacy, governance system	Women, women and girls, Working class communities, migrants and undocumented communities
Media	LGBTIQ community
Philanthropy, civic space (online and offline)	Disabled community, working class communities, migrants and undocumented communities
Bookseller and organiser	Women, women, and girls, LGBTIQ community, working class communities
Knowledge production	Women, LGBTIQ community
Business support services	Women, women, and girls, LGBTIQ community, working class communities
Gender and research	Women and girls
Philanthropy and human rights	LGBTIQ community
Sexual and reproductive rights	Women, LGBTIQ community
Sexual and reproductive services	Women, LGBTIQ community
Philanthropy	Women, women and girls, disabled community, working class communities, migrants and undocumented communities, children
Social media	Women, LGBTIQ community
Community manager	Women, women, and girls, LGBTIQ community, working class communities
Feminist internet rResearch	Women, LGBTIQ community, disabled community
Education - Human rights law	Women, LGBTIQ community

Ethical considerations for this study were based on feminist internet ethical research practices.¹⁴ These ethical principles were built as part of a collaborative process for feminist internet researchers. They draw from feminist politics and values and existing ethical requirements and frameworks for researchers. Feminist ethics take into account care, power dynamics, and approach that does not result in the extraction of data – but instead value building for participants to understand the related data harms. In thinking of consent in both interviews and surveys, the purpose of the study clearly explained the goals and purposes of the information

14 <https://genderit.org/resources/> (accessed 20 September 2020).

provided for the study. Consent could also be withdrawn at any time during the study. This was communicated to all participants at the start of engagement, during the research when they were responding and when the research was complete. At the completion stage, a draft research paper was shared with participants and they had the opportunity to review the work and consent to the final outcome or withdraw consent. In thinking of accountability in ethical practices – the researcher was accountable to the research participants. This was done through open communication on any potential harm and ensuring non-identifiable information would be captured. Power dynamics were also considered during the process such as institutional power dynamics and knowledge expertise of individuals participating. The design of the methodology opted for individual engagement as a better power balance dynamic.

3 Context

In its development, implementation, use and governance, technology is embedded in a context that frames existing social injustices. In this part we frame the social context that shapes the lived realities of women and gender-diverse marginalised groups.

3.1 Regional context: SADC region with a focus on South Africa

This research focuses on developing gender-responsive laws on data protection and privacy by looking at the sub-regional SADC model and South Africa as the country in focus. SADC currently has 16 members and focuses on ensuring sustainable economic growth through cooperation and ensuring peace and security so that the region may become a competitive world economic player.¹⁵ Gender equality forms one of the mainstreams of the region's policies with a strategy that aims to ensure equality and empowerment for women and girls. The 2008 SADC Gender and Development Protocol aims to deepen regional integration and strengthen community capacity in eliminating gender inequalities and marginalisation of women.¹⁶

Looking at digital development in the region – internet uptake in the region is relatively low at 22.3 per cent, with individual country uptakes ranging from 9,8 to 58,8 per cent. There are guiding legal and regulatory

15 40th SADC Summit 17 August 2020, https://www.sadc.int/files/4415/9760/6150/40th_SADC_Summit_Brochure_2020.pdf (accessed 30 September 2020).

16 SADC 'Gender mainstreaming' 2012, <https://www.sadc.int/issues/gender/gender-mainstreaming/> (accessed 30 September 2020).

frameworks to respond to digital development. The SADC Harmonised Cyber Security Legal and Regulatory Framework of November 2012 consists of three SADC Harmonised Cyber Security Model Laws that currently regulate e-transactions/e-commerce, data protection and cybercrime.¹⁷ The Digital SADC 2027 provides a blueprint for ICT infrastructure.¹⁸

South Africa is the leading economy in the region, and it was ranked the second largest economy on the continent, after Nigeria, in 2019.¹⁹ Despite this economic status, South Africa exists in the context of a triple threat of high inequality, poverty and unemployment, remnants of colonisation and apartheid. South Africa's inequality is steeped in layers of race, spatial distribution and gender, which impacts how its society experiences this triple threat.²⁰ Women represent approximately 51.2 per cent of the population in the country, yet there exists gender gaps in the income and labour market. Women are less likely to participate in the labour market than men.²¹ The gender wage gap is stark, with women's monthly earnings remaining around 70 per cent of men's earnings.²² The wage gap is further illustrated in the expenditure abilities of female and male-headed households. Male-headed households are better in terms of consumption and livelihood; female-headed households are at lower ends of expenditure deciles.²³

In addition to this economic inequality, gender-based violence disproportionately affects women, girls and non-gender conforming individuals such as lesbian, gay, bisexual, transgender and/or intersex people.²⁴ Gender-based violence in South Africa manifests itself as intimate partner violence and/or sexual violence and is usually perpetrated by men.²⁵ In the current health pandemic, together with having the

17 SADC Summit (n 15).

18 As above.

19 African Development Bank 'Southern Africa Economic Outlook' 2019, https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/2019AEO/REO_2019_-_Southern_africa.pdf (accessed 30 September 2020).

20 Statistics South Africa 'Inequality trends in South Africa' 2019, <http://www.statssa.gov.za/publications/Report-03-10-19/Report-03-10-192017.pdf> (accessed 30 September 2020).

21 As above.

22 As above.

23 African Development Bank (n 19).

24 Safer Spaces 'Gender-based violence South Africa' 2014, <https://www.saferspaces.org.za/understand/entry/gender-based-violence-in-south-africa> (accessed 30 September 2020).

25 As above.

highest recorded cases of COVID-19 infections on the continent, gender-based violence cases spiked as lockdown measures were instituted.²⁶ To understand the context of violence in South Africa, Pumla Dineo Gqola in 'Rape – A South African nightmare' highlights the complexity and societal attitudes towards which we may see rape as a norm and excuse it and, at the same time, the toxic masculinity discourse.²⁷

In terms of digital technologies, South Africa is also one of the leaders in internet use, with over half of the population (53 per cent) having access to the internet.²⁸ Connectivity is well developed in urban and semi-urban areas with gaps remaining in rural areas. Digital inequalities between men and women in South Africa reflect underlying inequalities in education and income, which impact access and use of the internet.²⁹

3.2 Digital rights: The right to privacy and data protection

Data feminism captures a wide understanding of social injustices and digital rights, but this chapter focuses on privacy and data protection. The concept of the right to privacy and data protection on the continent has steadily progressed over the last decade with laws developing at various times at national, sub-regional and regional levels. The African Declaration on Internet Rights and Freedoms accurately notes that 'many governments in Africa lack both the technical and legal resources to legislate appropriately and the political will to provide comprehensive protection to human rights in the context of internet and digital technologies'.³⁰ Where data protection laws do exist, they either replicate European law models or do not sufficiently protect and promote human rights and freedoms as they concentrate more on curbing cybercrime, terrorist activities, or curtailing criticism of governments.

The revised Declaration of Principles of Freedom of Expression and Access to Information adopted in 2019 provides guiding principles

26 The Presidency South Africa 'President Cyril Ramaphosa condemns surge in murders of women and children' 13 June 2020, <http://www.thepresidency.gov.za/press-statements/president-cyril-ramaphosa-condemns-surge-murders-women-and-children> (accessed 30 September 2020).

27 R Davis 'Review – Rape: South Africa nightmare' 2015, <https://www.dailymaverick.co.za/article/2015-09-25-review-rape-a-south-african-nightmare/> (accessed 30 September 2020).

28 A Gillwald 'After access: State of ICT in South Africa' 2018, https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf (accessed 28 September 2020).

29 As above.

30 <https://africaninternetrights.org/en/about> (accessed 30 September 2020).

on freedom of expression and access to information on the internet.³¹ Principles 40 to 42 focus on privacy and protection of personal information and place the onus on states to adopt laws for the protection of personal information in accordance with international human rights laws and standards. The guiding principles for privacy laws notably focus on the harmful sharing of non-consensual intimate images and prescribe that these offences should be punishable by law. The African Union (AU) also published the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) which contains provisions that must be adhered to once the Convention becomes legally binding.³² However, only 14 countries have signed the document, and only eight have ratified it.³³

The SADC Model Law on Data Protection (SADC Model Law) is a non-binding law developed as part of the Harmonisation of ICT Policies in sub-Saharan Africa (HIPSSA).³⁴ The South African Protection of Personal Information Act of 2013 (POPIA) came into full effect in July 2020, with a 12-month grace period for compliance. Its provisions are framed in a way that ensures compliance for regional and global business practices and provides for the collection, processing and use of personal information.³⁵

Table 2 provides insights on definitions of personal and sensitive data; consent; data subjects' rights that are covered in the laws; and how gender and sexuality are identified as categories of personal information in the SADC Model Law and POPIA. Gender and sexuality concerns are not fully engaged with in these laws, suggesting that justice may only be available to heteronormative and cisgender persons. In the SADC Model Law the processing of personal data relating to a data subject's sex life and, perhaps indirectly, gender identity is authorised, an alarming

31 The African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, <https://www.achpr.org/legalinstruments/detail?id=69> (accessed 29 September 2020).

32 African Union African Union Convention on Cyber Security and Personal Data Protection 2014, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (accessed 29 September 2020).

33 African Union List of countries which have signed, ratified, acceded to the African Union Convention on Cyber Security and Personal Data Protection 2020, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protectionUnion> (accessed 29 September 2020).

34 SADC Model Law on Data Protection, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 30 September 2020).

35 Protection of Personal Information Act 4 of 2013.

provision as it is to be done by an association with a legal personality or an organisation of public interests ‘whose main objective, according to its articles of association, is the evaluation, guidance and treatment of persons whose sexual conduct can be qualified as an offence’.³⁶ This clause is a challenge to gender and sexual minorities whose lifestyle may be considered deviant and, therefore, qualify as an offence. At the time of this research, concerns or criticisms of this clause were not found within the digital rights or queer community.

Table 2: Breakdown of selected data protection principles

Data protection principles	SADC Model Law	POPIA
Definition of data	Personal information relates to data subjects that is processing of an individuals’ personal data and who is identified or identifiable. Sensitive data is considered data that may reveal genetic data, biometric data, race, gender, and processing of data concerning health and sex life	Personal information means information relating to an identifiable, living, natural person, and, where it is applicable, an identifiable, existing juristic person. This also covers, race, ethnicity, language, health, and sexual orientation

36 SADC Model Law (n 34) sec 15 (4).

Consent	Consent refers to any manifestation of specific, unequivocal, freely given, informed expression of will by which the data subject or his/her legal, judicial, or legally appointed representative accepts that his/her personal data be processed. Processing of sensitive data requires written consent.	Consent means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information. The processing of personal data is only allowed with the data subject's consent or their parent or guardian if they are minors.
Purpose specification	Right to notice on purpose of data processed and whether compulsory or not.	Requirement that data be collected for a specific purpose and the person to whom the information relates must be notified when their data is being processed, must be able to access information on whether their data is being collected or processed, and must be able to object to the processing of their data.
Data security	Provisions of security in data collection and processing for data controller and processor	A data subject and the data Regulator must be notified of any security breaches
Purpose limitation	Data processed must be limited to what is necessary and not excessive.	Personal information may only be processed if it is adequate, relevant, and not excessive for the purpose it has been collected for. Further processing of information must be in line with the initial purpose of collection.

Retention	Data must be accurate and kept up to date, and the data subject must be informed of the purpose which it is collected	Information must not be retained any longer than necessary unless based on exemptions
Right to erasure	Right to rectification or erasure by bringing complaints to relevant authority free of charge	A data subject has the right to have their personal information corrected or deleted upon request
Right to be informed	Right to consent through an agent and right to object to processing	A data subject has the right to be notified when their personal information has been collected and is being processed.
Provisions for automated decision making	-	A data subject may not be subject to a decision with legal consequences solely on the basis of automated processing of personal information

3.3 Artificial intelligence discourse in the region

The discourse on AI in the region has been that of a developmental and economic growth paradigm based on the idea of the fourth industrial revolution.³⁷ Birhane describes the discourse of AI-based innovations in some circles being taken up with much enthusiasm as follows: ‘Mentions of “technology”, “innovation” and AI continually and consistently bring with them evangelical advocacy, blind trust and little, if any, critical engagement. They also bring with them invested parties that seek to monetize, quantify and capitalise every aspect of human life often at any cost.’³⁸

37 S Sanyal ‘AI to change the world in our lifetime’ 2018, <https://digitalskillsglobal.com/blog/ai-to-change-the-world-in-our-lifetime> (accessed 30 September 2020); T Marwala ‘Fourth industrial revolution: Let’s all work in a synchronised manner’ 2019, <https://www.uj.ac.za/newandevents/Pages/Fourth-Industrial-Revolution-Let%E2%80%99s-all-get-to-work-in-a-synchronised-manner.aspx> (accessed 18 January 2020).

38 A Birhane ‘Algorithmic colonisation of Africa’ (2020) 17 *SCRIPTed* 394.

schools dedicated to AI in Ghana, led by Moustapha Cisse.⁴² In Kigali, Rwanda, the African Institute for Mathematical Scientists (AIMS) is running a one-year Master's degree programme in partnership with Facebook and Google to create the next generation of tech leaders.⁴³ South Africa has the Centre for Artificial Intelligence Research, a university consortium focused on building research on AI.⁴⁴ Communities such as the Deep Learning Indaba have also emerged, which focuses on strengthening machine learning and AI in Africa. Their mission statement states they 'work towards the goal of Africa being not only observers and receivers of the ongoing advances in AI, but active shapers and owners of these technological advances'.⁴⁵

However, as these efforts escalate, so does the gender gap in STEM fields, which is an issue that impacts those participating in these processes. The 2018 AI Index reported that women are severely underrepresented in university faculties and, consequently, as candidates for jobs in the AI sector.⁴⁶ Women account for only 28 per cent of science researchers while men dominate at 72 per cent.⁴⁷ As Leavy points out, the overrepresentation of men in the design of AI and technologies could quietly undo decades of advances in gender equality.⁴⁸ In addition, the way in which AI is gendered often frames women in subservient positions such as using female names in voice recognition systems and using 'female personas' as digital assistants.⁴⁹

Policy conversations on AI-based innovations also focus on ensuring economic gains through the creation of employment opportunities,

42 K Lijadu 'How a Master's programme in machine intelligence is trying to close an African tech gap' 2018, <https://qz.com/africa/1344552/google-facebook-back-african-machine-intelligence-program/> (accessed 18 June 2020).

43 N Munyampenda 'AIMS launches African Master's in Machine Intelligence' 2018, <https://nexteinstein.org/aims-launches-first-of-its-kind-african-masters-in-machine-intelligence-at-rwanda-campus/> (accessed 18 June 2020).

44 <https://www.cair.org.za/> (accessed 30 September 2020).

45 Deep Learning Indaba, <https://deeplearningindaba.com/2020/> (accessed 15 June 2020).

46 Artificial Intelligence Index 2018 Annual report, <http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf> (accessed 30 September 2020).

47 <https://www.aasciences.africa/news/bridging-gender-gap-women-science-africa> (accessed 30 September 2020).

48 S Leavy 'Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning' (2018) Conference Paper 1st International Workshop on Gender Equality in Software Engineering, <https://doi.org/10.1145/3195570.3195580> (accessed 15 June 2020).

49 P Fung 'This is why AI has a gender problem' 2019, <https://www.weforum.org/agenda/2019/06/this-is-why-ai-has-a-gender-problem> (accessed 18 June 2020).

ensuring that citizens are upskilled to be ready for the revolution, being innovative enough to attract global business as well as being compliant enough for global trade. SADC is looking at AI in relation to the model law on the digital economy in development.⁵⁰ In South Africa, the policy focus is on AI and data diversity in different sectors as well as being responsive to global developments by building capacities for engagement.⁵¹ The focus on sector development has seen engagement from diverse departments, including trade, industry and competition, and communication and digital development. In its 2019 White Paper, the Department of Science and Information (DSI) focused on how emerging technologies, including AI, may be used for inclusive economic growth by capturing policy commitments to address poverty, inequality and unemployment.⁵² South Africa also put together the Fourth Industrial Revolution Commission (4IR Commission) to lead the way in the take up of technology and develop policies prioritised on inclusive economic growth.⁵³ The 2020 National Planning Commission report on Digital Futures assessing South Africa's readiness for the fourth industrial revolution provides insight into the readiness and the necessary policy interventions required to use these technologies for development.⁵⁴ Despite much of South Africa's AI and data-related policies and legislation being at a formative stage, the country's existing regulatory framework has relevance to both the current governance of data and AI, as well as the conceptualisation and interpretation of new policies in this space.

Critics have pointed out the current risk of perpetuating digital disparities and inequality in the discourse around AI.⁵⁵ Digital disparities in gender, for example, illustrate the inequality that women experience at the intersection of poverty, gender and unemployment. Based on the information we have on people's experiences with digital technologies

50 G Razzano 'RIA and SADC Parliamentary Forum co-host workshop on digital economy' 2020, <https://researchictafrica.net/2020/09/28/ria-and-sadc-parliamentary-forum-co-host-workshop-on-digital-economy/> (accessed 30 September 2020).

51 R Adams and others 'AI policy series 1: Can AI and data support a more inclusive and equitable South Africa?' (2020), https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData1_IntroSeries_Elec.pdf (accessed 15 September 2020).

52 <https://www.dst.gov.za/index.php/> (accessed 20 September 2020).

53 <https://www.gov.za/documents/> (accessed 28 September 2020).

54 National Planning Commission 'Digital futures: South Africa's digital readiness for the fourth industrial revolution' 2020, <https://www.nationalplanningcommission.org.za/assets/Documents/> (accessed 15 September 2020).

55 A Gillwald '4IR in SA is too important to remain the domain of the elite' 2019, <https://www.businesslive.co.za/bd/opinion/2019-07-04-4ir-in-sa-is-too-important-to-remain-the-domain-of-the-elite/> (accessed 14 June 2020).

‘these challenges in a data driven environment then represent a classical human development challenge’.⁵⁶ Given varying levels of gendered inequality, women may be the last to capture the benefits of the fourth industrial revolution.⁵⁷ Therefore, replicating existing inequalities, new social injustices and unequal power dynamics will impact the differences in experiences of these new technologies.⁵⁸

4 Gendered harms from AI-based systems

The reproduction of power asymmetries through automated decision-making systems shows that the rationality of computers or of humans programming the machines does not always take context into account.⁵⁹ As the implementation of AI systems takes place, the question of whether the region is ready to harness the opportunities they present while, at the same time, ensuring safeguards for human rights and, by extension, digital rights becomes critical. Socio-economic status, gender, ethnicity and geo-location all influence the way in which our data is treated in different contexts and influence decisions made from that context. In already unequal societies, AI and machine learning technologies may further perpetuate stereotypes and amplify injustices. In this part the gendered concerns are highlighted and the extent to which the SADC Model Law and POPIA may address these issues are discussed.

4.1 Data concerns – The right to privacy and data protection

The focus on AI harms begins with concerns around data through a feminist lens. While governments and technical communities are seeking or collecting enormous amounts of data to better their technologies, for users, concerns are around control and agency over their data. As the feminist principles of the internet highlight, agency is important to establish an internet that would transform gendered inequalities in society. The feminist principle of privacy and data focuses on the ability to have control over your information and to understand how it is being used, reject the ‘for profit only’ focus on data use and manipulative behaviour

56 A Gillwald ‘Data, AI and society’ 2020, <https://researchictafrica.net/2020/03/10/data-ai-society/> (accessed 30 September 2020).

57 R Adams ‘The fourth industrial revolution risks leaving women behind’ 2019, <https://www.weforum.org/agenda/2019/08/the-fourth-industrial-revolution-risks-leaving-women-behind/> (accessed 18 June 2020).

58 As above.

59 S Mhlambi ‘From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance’ (2020) *Carr Centre for Human Rights Policy* 2.

such as targeted advertisements.⁶⁰ Most narratives around data focus on it as if it were an entity that exists outside our personhood; however, data is a part of us, and our experiences of data and privacy embody the concept of 'data bodies'.⁶¹ Often, the language used in data protection laws, such as 'data subject', has a disembodying effect.

The right to privacy from a gender perspective is particularly important as 'with gender stereotypes comes problems of privacy invasion and abrogation'.⁶² Allen frames this as 'un-easy access', which helps in highlighting the way in which access to the internet may be problematic for women and gender-diverse people as the continuation of existing power dynamics and control from offline realities.⁶³ Power dynamics and control over data are seen in the disregard for agency as Privacy International's work highlights how period tracking applications collected and used intimate data and personal information for their monetary gain via third-party exchanges without informing their users.⁶⁴

Consent often is key when thinking of data and data protection for the rights of people, but when located in the current context, the question becomes – do people have the power, ability, and capacity to say no?⁶⁵ The SADC Model Law and POPIA focus on consent with regard to personal information being a specific informed expression. The SADC Model Law furthers consent in that it must be freely given and unequivocal – which provides language on the extent of what consent would be. In the context of inequality in the region, data concerns with regard to privacy and data protection are about people's capabilities and freedoms to achieve this and their capacity to aspire to privacy in constrained environments.⁶⁶

60 'Measuring digital development' (n 1).

61 A Kovacs 'When our bodies become data, where does that leave us?' 2020, <https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969> (accessed 28 September 2020); T Wang 'You are not your data but your data is still you' 2020, <https://deepdives.in/you-are-not-your-data-but-your-data-is-still-you-b41d2478ece> (accessed 30 September 2020).

62 A Allen 'Gender and privacy in cyberspace' (2000) 52 *Stanford Law Review* 1175.

63 As above.

64 <https://www.privacyinternational.org/> (accessed 20 August 2020).

65 P Pena & J Varon 'The ability to say no on the internet' 2019, <https://medium.com/codingrights/the-ability-to-say-no-on-the-internet-b4bdebf46d7> (accessed 30 July 2020).

66 P Arora 'Decolonising privacy studies' (2019) 20 *Television and News Media* 368.

4.2 Gender harms

The question often raised is what makes AI harms gender specific in a society of existent inequality. This part provides narratives around the specific privacy and data related harms for women and gender-diverse people in these contexts of inequality. The SADC Model Law and POPIA do not unpack the gender harms generally related to privacy violations and the language used in the laws is not gender representative. Gender is not fully engaged with as a possible category of harm; rather, it is sex life that is considered sensitive data. Article 15(4) of the SADC Model Law has already been flagged as a challenge to sexuality as it allows for processing information relating to a data subject's sex life if their behaviour is deemed harmful to society. In countries under the SADC region that have legal ramifications against sex life that is deemed inappropriate – often those of gender-diverse people – this raises concerns over how this information may be used for persecution. The model law does not define what would be considered 'harmful' to society. This area of work needs to be engaged within countries that may be developing their laws based on the SADC Model law.

South Africa has constitutional provisions against discrimination on the basis of sex or gender, the language in the POPIA contains gendered pronouns that are discriminatory to people who do not identify as 'he' or 'she'. The use of gender-inclusive legal drafting is not a new phenomenon. In South Africa, the Cybercrimes and Cybersecurity Bill [B 6 – 2017] is one of the first pieces of forthcoming legislation to incorporate the usage of gender-diverse language. The select committee reviewing recommendations of the Bill in 2020 agreed to '(a) altering the tone of the Bill to reflect non-binary language as required by considerations of gender-neutrality, equality, dignity and identity'.⁶⁷ This signifies the move from gender-neutral language to gender-inclusive language and may be built into how the data protection and privacy implementation may include gender-inclusive language.⁶⁸

The challenge in this study is that most of the examples of gender harm found exist in European and American contexts. There are few research pieces on the societal impact of this work. Loss of privacy, discrimination by gender or health, data breaches, and harms due to

67 Parliamentary Monitoring Group -ATC200617: Report of the Select Committee on Security and Justice on the Cybercrimes Bill [B 6B – 2017] (National Assembly – sec 75) (introduced as Cybercrimes and Cybersecurity Bill [B 6 – 2017]) dated 11 June 2020, <https://pmg.org.za/tailed-committee-report/4209/> (accessed 30 July 2020).

68 Arora (n 66).

machine or algorithm bias form some of the injustices in societies driven by data.⁶⁹ Race, ethnicity and biometric personal information are categories of protected sensitive personal data that are prohibited from processing in the SADC Model Law and POPIA. However, the harms that would need protection from are missing in legislation. For example, both laws do not mention privacy breaches and the subsequent use of technology to develop or distribute non-consensual images. Table 4 provides examples of some of the related harms this research has mapped over the course of the year from the European and American contexts.⁷⁰

Table 3: Gender-based harms related to artificial intelligence-based systems

Harm	Harm basis	Harm occurring
Discrimination	Social bias	AI relying on algorithms learnt from real-world data can inadvertently reinforce existing social biases.
Discrimination	Gender, weight, skin tone	The body imaging technologies now used in many airports around the world to screen passengers are often represented as objective and neutral, yet the aim of using such technologies is to police non-normative bodies which means that some bodies are more likely to be treated as a potential threat.
Publication and sharing of non-consensual explicit material	Gender	AI-generated fake videos (deep fakes) are becoming more common and, as with everything, women are being disproportionately affected by them as seen through deep fake porn.
Harassment	Malice, gender, gender identity	The use of targeted anti-LGBTQI+ ads on LGBTQI+ online platforms is malicious and psychologically harmful

69 J Redden & nd J Brand 'Data harm record' 2017, <https://datajustice.files.wordpress.com/2017/12/data-harm-record-djl2.pdf> (accessed 15 May 2020).

70 A mapping of gender harms related to artificial intelligence-based systems, https://mydatarights.africa/wp-content/uploads/2020/12/Data-Harms_2020.pdf (accessed 15 December 2020).

Stereotyping	Automated discrimination	The use of gendered ‘voices’ and ‘responses’ and the use of gendered pronouns and syntax tend to perpetuate harmful gender stereotypes.
Racism	Racial bias	AI technologies have also been guilty of racism - from misidentifying some of the most iconic black women in the present day, such as Michelle Obama, Serena Williams, and Oprah Winfrey, to labelling black people in images as gorillas, which is a racist trope.
Economic harm	Gender bias	There is evidence of targeted ads where algorithms are perpetuating the pay gap by targeting listings for better-paid jobs towards men.
Surveillance	Unauthorised surveillance	Contrary to international human rights law, governments are engaging more and more in mass surveillance, mostly merely because they can.
	Ethnicity and race	A range of interacting characteristics – race, ethnicity, religion, gender, location, nationality, socio-economic status – determine how individuals become administrative and legal subjects through their data and, consequently, how this data can be used to act upon them by policymakers or commercial firms. The possibility of being identified as a target of surveillance multiplies depending on the number of categories of interest one belongs to.

4.3 Perceived concerns of data harms

As there is very limited information on the experience of these harms on the African continent, in the survey AI scenarios were presented to participants, and they were asked to reflect on how these harms would play out in the South African context. The collection and processing of personal data is of great concern in terms of who has access to this

information (24 out of 25); the way in which this information will be used (22 out of 25), and where the information will be stored and processed (21 out of 25). In this context of data collection, processing and use, participants were concerned about how this data may be used to challenge their safety; the monetisation of this information; who has access to this information, especially when it is sensitive to sexual rights or sex work and discussions in the LGBTQI community. As one of the respondents pointed out: 'Harassment and the usage of our data [is a concern]. Privacy is of most importance in the work we do because we deal with people who are seeking terminations of pregnancy in a society with stigma. They want their information to be private and we use social media to do our work' (survey participant 1, 2020).

The current laws have provisions on data subjects' rights to be informed about their data collection, processing and use. The limitation with AI, however, is that the data sets are built up of non-identifiable data – it is this aggregate data with an impact on communities and individuals.

The second scenario focuses on monitoring activities leading to profiling that exposes one to targeted advertising. In this instance, all participants were aware of this activity and privacy and data protection was a great concern. Different concerns emerged because of monitoring online and this was related to the type of information they worked with – sensitive information or planned activities. In addition, activists were greatly concerned with how their location data seems easily available, influencing targeted advertising across platforms, yet this could mean they could also be targets for those against their work.

The participants raised concerns about how their location could be determined and the targeted advertising content they received based on how they had been profiled. One respondent pointed out that because of working on gender identities and sexualities, the advertisements or spam email they received was often in the form of harassment and/or violence. The adverts also perpetuate harmful stereotypes and prejudices. One of the most interesting insights was related to the access of reproductive rights – when women search for abortion services, it was pointed out that they seem to be directed to illegal abortion service providers – which disturbs access to safe abortions. POPIA, in section 69, focuses on the prohibition of targeted direct marketing by means of unsolicited electronic communication, but profiling for targeted advertising is not covered,⁷¹ while the SADC Model Law places an onus on the data controller

71 <https://popia.co.za/> (accessed 30 September 2020).

and processor for people to be informed of the right to object to direct marketing.⁷²

The third scenario focused on discrimination. The example highlighted how algorithms perpetuate the gender pay gap by showing better-paying jobs to men and employed the example of Amazon's hiring tool that was biased against women. Half of the respondents were aware that this was an issue. The majority, 18 out of 25 participants to be precise, were concerned about privacy and data protection in this context. As this was an example based in a different context, 22 out of 25 participants indicated this as important in the cases of South Africa. Race, ethnicity, location, citizenship, health status, digital connectivity, and gender were raised as potential points of discrimination in South Africa. These are personal information categories protected against discrimination. However, discrimination through the use of automated decision-making systems would have an impact on access to opportunities when one does not fit a particular profile. Five respondents raised racial and gender discrimination in accessing financial services as a major concern related to algorithm discrimination. One of the participants noted that 'it has been reported that this is a problem in the banking sector, where AI is racist and sexist. Black women will thus stand no chance when applying for loans. I would be surprised if one's geographical location does not automatically exclude many from opportunities. Of concern are people from the rural areas, townships, informal settlements, and crime-infested areas' (survey participant 2, 2020).

The categorisation of data into sensitive and non-sensitive data is a recurring feature in most data protection legislation. Yet, through processes such as profiling, detailed and highly-comprehensive profiles can be developed from what is seemingly unimportant or 'non-sensitive' data. Profiles are used to make automated and consequential decisions such as hiring, credit scoring or national security. Therefore, as much as data regulation allows you to object to the use of your data or the right to know how your data is being used, it cannot account for issues emerging with AI.

Section 71 of POPIA provides for people not to be subject to the automated processing of personal information intended to provide a profile of such a person, including their performance at work or their creditworthiness, reliability, location, health, personal preferences or conduct. This clause is important in addressing the issues raised of discrimination and bias concerning access to South Africa's financial

72 SADC Model Law (n 34).

services. However, there is a need for the assessment of automated processing of personal information and transparency reports from organisations that make use of these systems and how they impact gender and sexual minorities.

The fourth scenario focused on surveillance by drawing on the roll-out of closed-circuit television (CCTV) or surveillance cameras and facial recognition systems in South Africa. There was a high level of awareness of this roll-out, and 73 per cent of the participants found this to be a relevant issue of privacy and data. Two issues were highlighted as the most significant for participants – 20 of the participants were concerned about how the technology may be used to invade their privacy and, at the same time, 16 participants saw the usefulness of surveillance cameras to address crime. This issue was highlighted as a need to balance security and privacy. Other issues of concern in the South African context connected to surveillance were bias, discrimination and misuse of data for purposes of profiling. This was a concern in a country where police brutality is rife – this technology could be used for further discrimination and violence towards individuals. Race was a big underlying concern as these technologies may be used to profile black people in areas of wealth as un-belonging and, therefore, criminal. One participant indicated that ‘crime is associated with mainly blacks, in most instances viewed to be a result of foreigners and the collection of these images might be reinforcing a stereotypical approach to crime fighting. Second, I have no idea who is collecting and analysing the footage and what is the period of data retention. In the absence of enforcement provisions and powers of the Information Regulator until 2021, it means that there are few remedies at all’ (survey participant 3, 2020).

The final fifth scenario presented issues of privacy and data protection in relation to gender identities and sexual orientation. The example used focused on how a privacy breach may expose someone’s sexual orientation and the impact of location data being used to locate victims of gender-based violence. All the participants were aware of this as an issue. Ninety per cent of the participants were concerned about their privacy in this context and found it relevant to their work area. For 24 out of 25 of the participants this was a concern and they wanted to know how to address this issue. The concerns with privacy breaches were related to how this information may be used. An example given was how women’s health information, if exposed to a data breach, may be used for problematic targeted advertisement. One of the participants indicated that a ‘privacy breach can also make someone susceptible to revenge porn, online initiated human trafficking and kidnappings of women, children and sexual minorities’.

Key contextual issues that were recurring references were race, economic status, homophobia and gender-based violence. The issues around bias, discrimination and increased surveillance were raised as likely to be of concern as well. This raised questions of security breaches and their online safety given the sensitivity of their work. Safety and security concerns were raised in the context of the high levels of gender-based violence in South Africa. Despite the rights of the lesbian, gay, bisexual, transgender, queer/questioning and intersex (LGBTQI) community being protected, bias and discrimination will continue in these technologies with the reality of societal homophobia. In this instance the question of the extent to which anonymity can be guaranteed online is important.

As AI-based solutions emerge, the concern with regard to gender is not necessarily a direct identification but rather the emerging profiling and the targeted content based on that gendered profile. Even when data may be de-identified, algorithms may still be able to determine gender and sex life. Therefore, it is important to take necessary security safeguards that explicitly address these issues. Privacy impact assessments and other mechanisms of accountability would need to ensure that data analytics do not lead to inferences of individuals or groups related to gender leading to discrimination.

5 A gender-responsive policy action and the role of civil society towards privacy and data protection

This research provides a contextual understanding of AI, privacy and data protection with regard to gender. Civil society has a role to play in ensuring a gender-responsive privacy and data protection legal framework that ensures justice. The limitation of privacy and data protection laws stems from a general need to engage with the opportunities and challenges of AI-based innovations and, at the same time, a lack of general engagement with gender and privacy issues – a space that the civil society and activist community with which this research engage actively focus on. This part responds to the main research question by providing recommendations on gender-responsive law and policy from a feminist perspective to ensure data justice.

The context of gendered inequality based on income, education and gender-based violence, for example, highlights a need for more commitment on the impact AI would have on marginalised groups. Online violence is an issue for privacy and data protection and requires frameworks that address gender-based violence as a continuum of online-offline harms.⁷³ There is

73 Parliamentary Monitoring Group (n 67).

the need for the right to privacy and data protection to be fostered in a way that defines sensitivities and harms associated with intersex, transgender, and diverse communities.⁷⁴ This factors in data feminist principles of rethinking binaries and ensures justice by basing law reflective of lived experiences. Civil society actively engaged in the work on social justice issues may play the role of nuancing context on gendered injustices and how the law may be implemented cognisant of these issues. Civil society organisations may also collaborate with the academia to document harms and conduct research in order to build the necessary evidence base.

The design and implementation of the law should take into consideration the experience of injustice in different domains of power, which means that, even when the above categories are recognised, they do not take on a homogenised approach to ensuring privacy and data protection. Civil society and activists that work in these spaces may serve as friends of the policy makers and expert advisors to indicate the right language and approach to embedding safeguards for these issues into law and policy. They would also need to be resourced to build capacity to understand gender issues.

A responsive law also considers power dynamics, control and agency. This is a challenge in AI-based innovations where one is aware of privacy violations yet is uncertain on how to exercise these rights, leading to a digital inequality paradox. The ability to exercise your rights online depends on awareness of the issue, digital skills and literacy, and being able to use the internet meaningfully and understand how your data will be used. The concern is that without the ability to do this, one loses their agency. This requires placing an onus on those who collect the data to bear the cost and burden of explaining how the data is used in a way that is unequivocally understandable and considers accessibility barriers as well. The right to be informed needs to extend to use of AI – the significance for the envisaged processing, the challenges associated with it and the safeguards connected with its processing. The success of a responsive law would require working with civil society in creating awareness and capacity-building campaigns with marginalised groups so that they may be able to advocate for their rights. Adequate resourcing from the state or the donor community is important for this to be successful. The more people are informed about their rights, the quicker it is to flag data abuses and violations and the more input from multiple sectors on how to improve data protection.

74 United Nations Report of the Special Rapporteur on the right to privacy (2018), <https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx> (accessed 20 May 2020).

Auditing systems of harms are crucial, and gender should be a key consideration. Data protection impact assessments that consider gender dynamics would also be an important tool for ensuring data justice. This involves identifying, evaluating and addressing the impacts on data subjects and their personal data of a project, policy, programme, or other initiative that entails processing such data.⁷⁵ In addition, states and non-state parties could provide easy access to data profiles and monitoring for gender bias.⁷⁶ Most algorithms are like black boxes, which impacts understanding of what is provided or incorporated. Principles of fairness, explainability, auditability, responsibility and accuracy should be infused. If this is done, it might reduce elements of bias. Automated decisions should also be explained, especially in financial-related transactions, as they may perpetuate inequality and exclusion when based on historical data. Public awareness campaigns must be conducted regularly and civil society should be meaningfully engaged in developing these systems of review. Civil society and activists are in a great position to help draft ethical conducts and privacy policies with research institutes, given their engagement and connection with affected groups. However, power dynamics may challenge the meaningful engagement of civil society in the process. Therefore, it is important to have adequate resources so that they make independent decisions without any interference from the technical community.

6 Conclusion

Placing gender and sexuality at the forefront of privacy and data protection ensures gender-responsive laws and policies. The current inequality in society affects women and the gender diverse communities adversely and extends to the digital space. The narrative of AI for development and economic growth may overlook the reality of gendered inequalities and increase them further. By taking on a feminist conceptual framework, this research has highlighted the challenges specific to women and gender-diverse people in society and how this is a continuum with digital technologies. The development of AI follows the trend of excluding gender diverse people in developing and implementing these innovations. While it is commendable that the right to privacy is recognised and data protection measures are in place, the limitations on how gender is applied to the policies indicate the need for more engagement of gender in policy and law development. The review of gender-specific harms related to privacy and data protection shows that a heteronormative

75 <https://www.icrc.org/en/data-protection-humanitarian-action-handbook> (accessed 28 September 2020).

76 (n 74).

and homogenous approach to policy is insufficient. Specific to AI, the awareness and concerns drawn from the survey indicate a concern in the processing, collection and use of data and the subsequent harms resulting from the algorithm nudges on these platforms.

To be gender-responsive eminently means to design and implement policies that take into account the gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development. This research provides a snapshot of these issues and starting points of actions led by civil society to having gender-responsive laws responsive to the needs of marginalised communities.

References

- Adams, R, Fourie, W, Marivate, V & Plantinga, P 'AI policy series 1: Can AI and data support a more inclusive and equitable South Africa?' (2020), <https://policyaction.org.za/> (accessed 15 September 2020)
- Allen, A 'Gender and privacy in cyberspace' (2000) 52 *Stanford Law Review* 1173
- Arora, P 'Decolonising privacy studies' (2019) 20 *Television and News Media* 368
- Birhane, A 'Algorithmic colonisation of Africa' (2020) 17 *SCRIPTed* 393
- Collins, PH *Intersectionality as critical social theory* (Duke University Press 2019)
- Crenshaw, K 'Mapping the margins: Intersectionality, identity politics, and violence against women of colour' (1991) 43 *Stanford Law Review* 1242
- D'Ignazio, C & Klein, FL *Data feminism* (The MIT Press 2020)
- Davis, R 'Review – Rape: South Africa nightmare' 2015, <https://www.dailymaverick.co.za/> (accessed 30 September 2020)
- Dencik, L and others 'Working paper: A conceptual framework for approaching social justice in the age of datafication' 2018, <https://datajusticeproject.net/> (accessed 18 June 2020)
- Fraser, N 'Abnormal justice' (2008) 34 *Critical Inquiry* 395
- Fung, P 'This is why AI has a gender problem' 2019, <https://www.weforum.org/> (accessed 18 June 2020)
- Gillwald, A '4IR in SA is too important to remain the domain of the elite' 2019, <https://www.businesslive.co.za/> (accessed 14 June 2020)
- Gillwald, A 'After access: State of ICT in South Africa' 2018, <https://researchictafrica.net/> (accessed 28 September 2020)
- Gillwald, A 'Data, AI and society' 2020, <https://researchictafrica.net/> (accessed 30 September 2020)
- Hussen, TS "'All that you walk on to get here": How to centre feminist ways of knowing' 2019, GenderIT <https://genderit.org/editorial/> (accessed 28 September 2020)
- Kovacs, T 'When our bodies become data, where does that leave us?' 2020, <https://deepdives.in/> (accessed 28 September 2020)
- Leavy, S 'Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning' (2018) Conference Paper: 1st International Workshop on Gender Equality in Software Engineering <https://doi.org/10.1145/3195570.3195580>

- Lijadu, K 'How a Master's programme in machine intelligence is trying to close an African tech gap' 2018, <https://qz.com/africa/> (accessed 18 June 2020)
- Marwala, T 'Fourth Industrial Revolution: Let's all work in a synchronised manner' 2019, <https://www.uj.ac.za/> (accessed 18 January 2020)
- Mhlambi, S 'From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance' (2020) *Carr Centre for Human Rights Policy* 1
- Munyampenda, N 'AIMS launches African Master's in Machine Intelligence' 2018, <https://nexteinstein.org/> (accessed 18 June 2020)
- Pena, P & Varon, J 'The ability to say no on the internet' 2019, <https://medium.com/> (accessed 30 July 2020)
- Razzano, G 'RIA and SADC Parliamentary Forum co-host workshop on digital economy' 2020, <https://researchictafrica.net/> (accessed 30 September 2020)
- Redden, J & Brand, J 'Data harm record' 2017, <https://datajustice.files.wordpress.com/> (accessed 15 May 2020)
- SADC 'Gender mainstreaming' 2012, <https://www.sadc.int/issues/gender/gender-mainstreaming/> (accessed 30 September 2020)
- SADC Model Law on Data Protection, <https://www.itu.int/en/ITU-D/> (accessed 30 September 2020)
- Safer Spaces 'Gender-based violence South Africa' 2014, <https://www.saferspaces.org.za/> (accessed 30 September 2020)
- Sanyal, S 'AI to change the world in our lifetime' 2018, <https://digitalskillsglobal.com/> (accessed 30 September 2020)
- Statistics South Africa 'Inequality trends in South Africa' 2019, <http://www.statssa.gov.za/> (accessed 30 September 2020)
- Tamale, S *Decolonisation and Afro-feminism* (Daraja Press 2020)
- Tandon, A 'Feminist methodology in technology research: A literature review' 2018, <https://cis-india.org/internet-governance/> (accessed 28 September 2020)
- Taylor, L 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4 *Big Data and Society* 1
- Wambui, J 'An introduction to feminist research' 2013, <http://erepository.uonbi.ac.ke/> (accessed 28 September 2020)
- Wang, T 'You are not your data but your data is still you' 2020, <https://deepdives.in/> (accessed 30 September 2020)

8

DATA PROTECTION AND PRIVACY FOR SOCIAL ASSISTANCE BENEFICIARIES: A SOUTH AFRICAN PERSPECTIVE

Ntando Ncamane

Abstract

Social Security plays a significant role in South Africa by ensuring that everyone has the right to social assistance, as enshrined in section 27 of the Constitution. In realising this right the legislature enacted the Social Assistance Act and the South African Social Security Agency Act, in which the former makes provisions for the different type of social assistance and the latter provides for the establishment of the SASSA, an institution responsible for the administration and payment of social assistance. Owing to the forever-evolving technology and the convenience it sometimes brings, the agency decided to migrate to digital payments of social assistance through SASSA master cards. In terms the law, the state is under the obligation to ensure that it protects personal information belonging to social assistance beneficiaries which is required by state for purpose of processing. The state is also under the obligation to guard against any illegal use of social assistance beneficiaries personal data. However, during the migration to digital payment SASSA breached laws which protects the data and privacy of the beneficiary. This is also evident in the landmark case of *Black Sash Trust v Minister of Social Development*, which validated the importance of the beneficiary's privacy and data protection. To this effect, the court ordered that the state, in particular SASSA, has a duty to protect information belonging to the social assistance beneficiaries and should devise measures that will protect personal information and deter any possible breach or illegal use. This chapter recommends sound and practical measures that can be adopted by the state so to circumvent any possible breach and illegal use of personal information belonging to social assistance beneficiaries.

1 Introduction

One of the signature achievements of our constitutional democracy is the establishment of an inclusive and effective programme of social assistance. It has had a material impact in reducing poverty and inequality and in mitigating

the consequences of high levels of unemployment. In so doing, it has given some content to the core constitutional values of dignity, equality.¹

The Constitution of the Republic of South Africa² makes provision for everyone to have the right of access to social assistance.³ This right falls under the socio-economic category of rights, among others, the rights to adequate food, water and social security.⁴ In *Government of the Republic of South Africa & Others v Grootboom & Others (Grootboom)*⁵ it was held that socio-economic rights are targeted at the vulnerable, and that government policies must be aligned to address socio-economic rights-related issues.⁶ The Court further stated that if the state has programmes in place to provide social assistance to citizens, the state has realised its obligation to realise socio-economic rights.⁷ In a bid to realise and distribute social assistance, the legislature has enacted the Social Assistance Act 13 of 2004,⁸ which provides for the rendering of social assistance services that the administration and payment of social grants.⁹ The South African Social Security Agency Act 9 of 2004¹⁰ was also enacted, giving rise to the establishment of the South African Social Security Agency with the duty to administer and monitor social grant payments.¹¹

South African technology has over the years evolved, and the South African Social Security Agency (SASSA) has been a beneficiary of these technological developments, such as the digitisation of payment of social grants, which included the introduction of smart cards, referred to as SASSA master cards. This endeavour was also meant to eliminate fraud related to the payments of social grants.¹² As a result, the services of cash payment services (CPS) were sourced to distribute social grant payments. The processing of payments requires the details of beneficiaries, and to

1 *Black Sash Trust v Minister of Social Development & Others (Freedom Under Law NPC Intervening)* (CCT48/17) [2017] ZACC 20; 2017 (9) BCLR 1089 (CC) (15 June 2017) para 1.

2 Constitution of the Republic of South Africa, 1996.

3 Sec 27(1)(c) Constitution.

4 Sec 27 Constitution.

5 2001 (1) SA 46 (CC).

6 *Grootboom* (n 5) para 36.

7 As above.

8 Social Assistance Act 13 of 2004.

9 Sec 3 Social Assistance Act.

10 South African Social Security Agency Act 9 of 2004.

11 Sec 2 South African Social Security Agency Act.

12 <https://www.gov.za/ten-million-sassa-mastercard-cards-issued-south-african-social-grant-beneficiaries> (accessed 15 September 2020).

protect their personal data and privacy, a legal framework was put in place to protect these beneficiaries from the illegal use of their personal information. The first of its kind is section 14 of the Constitution,¹³ which bestows the right privacy on everyone.¹⁴ The Protection of Personal Information Act 4 of 2013¹⁵ was enacted for public and private institutions to promote the protection of personal information. Furthermore, the South African Social Security Agency Act makes provision for SASSA to protect confidential information at its disposal.¹⁶ The duty of SASSA to provide adequate safeguards was confirmed in the landmark case of *Black Sash Trust v Minister of Social Development*.¹⁷ It further stated that it

contains adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004 ... Preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹⁸

The state's onerous endeavour to put in place a legal framework to enable the protection of personal data and privacy of social grant beneficiaries is commendable and has ameliorated the social assistance digitalised payment system. However, some notable shortcomings remain, which may defeat the purpose of the aforementioned legal measures that aim at the protection of beneficiaries. The first is non-compliance with the order of the Constitutional Court, also highlighted by the Black Sash that discovered, when making submissions to the UN General Assembly, that personal information that belongs to beneficiaries is still withheld by Net1, which contracted to CPS,¹⁹ which is contrary to the order of the Court quoted above. An article by Prinsloo and Ntondini suggests that there are still numerous cases of social grant personal data and privacy being used and, as a result, there are discrepancies in amounts paid to these beneficiaries.²⁰ Lastly, the SASSA and the South African Post Office (the new distributors of grants) personnel have not been fully acquainted with

13 Sec 14 Constitution.

14 Sec 14(1) Constitution.

15 Protection of Personal Information Act 4 of 2013.

16 Sec 16 SASSA Act .

17 *Black Sash Trust* (n 1).

18 *Black Sash Trust* (n 1) paras 76, 10.1.

19 Black Sash Submission UN General Assembly on Digital Technology, Social Protection and Human Rights 2019.

20 T Prinsloo & S Ntondini 'The exploitation of South African Social Security Agency grant recipients' data' (2006) *International Journal of Social Welfare* 16.

this new system, resulting in maladministration enabling cyber criminals to gain access to personal data of beneficiaries. This does not only have a negative impact on beneficiaries' personal data but also denies them the right to social assistance.²¹

It is against this background that this chapter will first examine the regulation of social assistance, in particular section 27(1)(c) of the Constitution,²² the Social Assistance Act 13 of 2004²³ and the South African Social Security Agency Act 9 of 2004,²⁴ which gave rise to the establishment of SASSA as the sole agency responsible for the payment of social assistance grants.²⁵ This chapter will further examine the laws put in place to protect social grant beneficiaries against the illegal use of data and the infringement of their privacy. These laws include section 14 of the Constitution,²⁶ which guarantees everyone the right to privacy. It will further examine the state's duty, in particular SASSA's duty, to implement safety measures in order to protect personal data and the privacy of social assistance beneficiaries when making payments, in light with the above-mentioned statutes. A brief analysis of the *Black Sash Trust* case²⁷ will be analysed as it contains safety measures to protect information pertaining to social assistance beneficiaries against the illegal use of their personal information. This safety is also extended to third parties who have been awarded a tender to render social assistance payments, which would require the personal details of the beneficiaries in order to effect payment. Lastly, the chapter will recommend solutions to the shortcomings associated with cash payment system inadequacies of beneficiaries' personal data and privacy.

2 Regulation of social assistance

Social assistance enjoys regulation and protection from the Constitution as well as other statutes, such as the Social Assistance Act and South African Social Security Agency Act. It is imperative for this study to first briefly define the terms 'social security' and 'social assistance' to gain a better understanding of the discussion that will follow.

21 B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development* 2017 (9) 1089 (CC)' (2019) 136 *South African Law Journal* 129.

22 Sec 27(1)(c) Constitution.

23 Social Assistance Act 13 of 2004.

24 South African Social Security Agency Act 9 of 2004.

25 Sec 2 South African Social Security Agency Act.

26 Sec 14 Constitution.

27 *Black Sash Trust* (n 1).

Social Assistance is defined in the White Paper on Social Welfare as ‘non-contributory and income-tested benefits provided by the state to groups such as people with disabilities, elderly people and unsupported parents and children who are unable to provide for their own minimum needs’.²⁸

In South Africa, social assistance has taken the form of social grants. Social assistance is a stream of social security law, which is defined by the International Labour Organisation (ILO) as ‘the protection that a society provides to individuals and households to ensure access to health care and to guarantee income security, particularly in cases of old age, unemployment, sickness, invalidity, work injury, maternity or loss of a breadwinner’.²⁹

Among the streams of social security there are other streams such as social insurance, social relief and private saving, which feeds up to the broad scope and purpose of social security law. Social security is covered by section 27 of the Constitution,³⁰ which means that social assistance has since enjoyed constitutional protection afforded in the new democratic dispensation. Section 27 of the Constitution³¹ reads as follows:

- (1) Everyone has the right to have access to –³²
 - (a) healthcare services, including reproductive health care;³³
 - (b) sufficient food and water³⁴; and
 - (c) social security, including, if they are unable to support themselves and their dependants, appropriate social assistance.³⁵
- (2) The state must take reasonable legislative and other measures, within its available resources, to achieve the progressive realisation of each of these rights.³⁶

28 Department of Welfare *White Paper for Social Welfare: Principles, guidelines, recommendations, proposed policies and programmes for developmental social welfare in South Africa* (1997) 50.

29 https://www.ilo.org/wcmsp5/groups/public/---dgreports/dcomm/documents/publication/wcms_067588 (accessed 15 September 2020).

30 Sec 27 Constitution.

31 As above.

32 Sec 27(1) Constitution.

33 Sec 27(1)(a) Constitution.

34 Sec 27(1)(b) Constitution.

35 Sec 27(1)(c) Constitution.

36 Sec 27(2) Constitution.

(3) No one may be refused emergency medical treatment.³⁷

The focal point of this study is on section 27(1)(c) which bestows on everyone the right to social assistance who is unable to support themselves, including their dependants. The state is required to take reasonable legislative measures within its resources to address social assistance concerns. The *Grootboom* case³⁸ acknowledges the dire need for the state to address socio-economic conditions in our societies as a result of the severe injustices of the past.³⁹ However, the Court was cognisant of the fact that the state might not be able to go beyond its limited resources in a bid to address socio-economic needs or to immediately realise these socio-economic rights. Notwithstanding the limitation on the realisation of socio-economic rights, the Court held that this was an explicit obligation and that the courts should at all times enforce these rights to enable the realisation of the rights.⁴⁰ The Constitutional Court in the case of *Khosa v The Minister of Social Development & Others; Mahlaule & Others v The Minister of Social Development & Others*⁴¹ highlighted the importance of social security but in particular social assistance, that the primary purpose of social assistance is that the state values human beings and it is to a social intervention for citizens to afford the basic life that they are not able to afford.⁴² To give effect to the constitutional mandate of the state, which is to provide social assistance, the legislature enacted the Social Assistance Act 9 of 2004⁴³ and the South African Social Security Agency 3 of 2004.⁴⁴ These two legislations had a tremendous impact towards the development of South African social assistance system. The Social Assistance Act was aimed at providing for the payment of social assistance grants and to outline the minimum requirements for persons to qualify for social assistance grants. The Act made provision for social assistance payments to be paid in terms of a child support grant;⁴⁵ a dependency grant;⁴⁶ a

37 Sec 27(3) Constitution.

38 *Grootboom* (n 5).

39 *Grootboom* (n 5) para 93.

40 *Grootboom* (n 5) para 94.

41 2004 (6) BCLR 569 (CC).

42 As above.

43 Social Assistance Act 9 of 2004.

44 South African Social Security Agency 3 of 2004.

45 Sec 4(a) Social Assistance Act.

46 Sec 4(b) Social Assistance Act.

foster child grant;⁴⁷ a disability grant;⁴⁸ an older person's grant;⁴⁹ a war veteran's grant;⁵⁰ and a grant-in-aid.⁵¹ Each category of social grant had its own eligibility requirements. The Act empowered the agency to make payments to persons who have submitted relevant information and meet the stipulated requirements. Primary to the South African Social Assistance Act was the provision for SASSA, which was entrusted with the responsibility of administering and paying social grant payments.

3 Regulatory framework to protect data and privacy of beneficiaries

3.1 International instruments

Sweden is regarded as the first country in the universe to enact data protection laws dating back to 1973. However, in the mid 1980s data protection was a global phenomenon as a result of there being a rapid emergence of the global market, leading to an increase in the exchange of personal information. This encouraged many international organisations to enact international instruments that will give rise to the protection of data and privacy.⁵² To regulate and provide guidance nations on matter of data protection and privacy, international organisations such as the Organisation for Economic Cooperation and Development (OECD), the European Council and the European Economic Community (now the European Union) (EU) came up with documents aimed at developing standard international data protection laws and to enable the free flow of information and also to archive uniform national laws on data protection and privacy.⁵³ The European countries under the Europe Council were the first to develop and enhance data protection and privacy laws. This is why many countries around the world draw lessons from EU countries, in particular the United States.⁵⁴

In 1990 the United Nations General Assembly (UNGA) adopted the Guidelines for the Regulation of Computerised Personal Data Files. The Guide provided the procedures for the implementation and proper

47 Sec 4(c) Social Assistance Act.

48 Sec 4(d) Social Assistance Act.

49 Sec 4(e) Social Assistance Act.

50 Sec 4(f) Social Assistance Act.

51 Sec 4(g) Social Assistance Act.

52 A Roos 'Core principles of data protection law' (2006) 39 *Comparative and International Law Journal of Southern Africa* 103.

53 As above.

54 Roos (n 52) 105.

guidance on data protection on national legislation of member states.⁵⁵ The Guidelines outline minimum guarantees to which member states should adhere. These minimum guarantees are the principle of lawfulness and fairness; the principle of accuracy; the principle of the purpose-specification; the principle of interested person access; the principle of non-discrimination; the power to make exceptions; the principle of security; supervision and sanctions; trans-border data flows; and fields of application.⁵⁶ However, the focal point of this chapter rather is on African data protection-related instruments. Hence there will be no further deliberation on EU instruments as this will serve no purpose.

The Social Protection Floors Recommendation 202 of 2012 was enacted to give guidance to member states to develop a comprehensive social security and extend social security coverage.⁵⁷ The Recommendation mandates member states to establish legal frameworks that will ensure that data of social security beneficiaries is legally protected.⁵⁸

Moreover, at the continental level, the African Union (AU), in a bid to curb cybercrimes and to protect personal data, has enacted the African Union Convention of Cyber Security and Personal Data Protection which was adopted in 2014.⁵⁹ The Convention comes after protracted deliberation from the first extraordinary meeting of African ministers who were responsible for communications resolute on a declaration that was directed at the AU to develop a continental cybersecurity and personal data protection as well as any other relevant needs of the continent. The Convention was adopted by the AU heads of state in 2014.⁶⁰ Chapter 2 of the Convention deals in detail with the regulation of personal data.⁶¹ As part of the Convention's objectives it encourages state parties to commit to establishing a legal framework that enhances the protection of personal data and to sanction those who breach privacy protection laws, without impeding the free flow of personal information.⁶² The Convention makes

55 UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, <https://www.refworld.org/docid/3ddcafaac.html> (accessed 27 November 2020).

56 As above.

57 Preamble to the Social Protection Floors Recommendation 2012 (No 202).

58 IV Monitoring of the Social Protection Floors Recommendation, 2012 (No 202) para 23.

59 African Union Convention of Cyber Security and Personal Data Protection 2014.

60 UJ Orji *The African Union Convention on Cybersecurity: A regional response towards cyber stability?* (2018) 98.

61 Ch 2 Personal Data Protection.

62 Art 8(1) African Union Convention of Cyber Security and Personal Data Protection 2014.

provision for member states to establish institutional frameworks for the protection of personal data.⁶³ The national authority of personal data is therefore tasked with the responsibility of being impartial and independent, which will ensure that data processing complies with the provisions of the African Union Convention of Cyber Security and Personal Data Protection.⁶⁴

The Convention goes further by outlining governing principles to the processing of data. It lists a number of principles, namely, the principle of consent and legitimacy of personal data processing;⁶⁵ the principle of lawfulness and fairness of personal data processing;⁶⁶ the principle of purpose, relevance and storage of processed personal data;⁶⁷ the principle of accuracy of personal data;⁶⁸ the principle of transparency of personal data processing;⁶⁹ the principle of confidentiality; and security of personal data processing.⁷⁰ The person, among other obligations owing to the data subject, the data controller, has an obligation to keep the processing of data confidential and the processing shall be performed by a person operating under the instruction of the personal data controller.⁷¹ The data controller is required to take all precautionary possible measures to ensure that personal data belonging to the data subject is not extinguished or tampered with by non-authorised persons.⁷² To amplify the protection of data and privacy in Africa, the Convention mandates the African Union Commission to develop guidelines on personal data protection. The guides were developed together with the Internet Society as well experts in the field of data protection and privacy, including privacy specialists,

63 Art 11(1) African Union Convention of Cyber Security and Personal Data Protection 2014.

64 As above..

65 Art 13, Principle 1 African Union Convention of Cyber Security and Personal Data Protection 2014.

66 Art 13, Principle 2 African Union Convention of Cyber Security and Personal Data Protection 2014.

67 Art 13, Principle 3 African Union Convention of Cyber Security and Personal Data Protection 2014.

68 Art 13, Principle 4 African Union Convention of Cyber Security and Personal Data Protection 2014.

69 Art 13, Principle 5 African Union Convention of Cyber Security and Personal Data Protection 2014.

70 Art 13, Principle 6 African Union Convention of Cyber Security and Personal Data Protection 2014.

71 Art 20 African Union Convention of Cyber Security and Personal Data Protection 2014.

72 Art 21 of the African Union Convention of Cyber Security and Personal Data Protection 2014.

academics and civil society groups.⁷³ The guidelines put an emphasis on ensuring that trust is paramount on online services to enable the digital economy to be beneficial and productive. The guidelines further emphasised the need for countries to create proactive measures so as to guard citizens against the victimisation of their personal data and to not disregard the role of other stakeholders in this regard.⁷⁴

Greenleaf and Cottier submit that Africa has made significant progress with regard to the advancement of the data protection laws. This is proven by the fact that the enactors of international instruments and national laws relating to data protection are countries in the European Council,⁷⁵ but Africa is leading on the expansion of data laws, which is evident from the fact that 12 countries have since 2013 adopted new laws. Most African countries have been first to apply to the European Council to be accepted to accede. Therefore, these factors should be evidence enough to prove data protection progression in Africa.⁷⁶

3.2 Constitution of the Republic of South Africa

The legal point of departure in the protection of data and privacy is the constitutional protection afforded to all beneficiaries of social assistance grants. Following the new democratic dispensation, the Constitution is viewed as being the supreme law and any law or act inconsistent with it is invalid.⁷⁷ The Bill of Rights, as the cornerstone of our democracy, guarantees everyone the right to privacy, which is the crucial right for purposes of this chapter. The case of *Bernstein v Bester*⁷⁸ remains a leading case that deals with the overall aspects of the right to privacy as far as South African jurisprudence is concerned. The case drew most of its inferences from foreign law to denote two fundamental approaches that should be taken into account where there is a dispute pertaining to the right to privacy. However, these approaches were based on what is termed as 'legitimate expectations'. The Constitutional Court held that 'it seems to be a sensible approach to say that the scope of a person's privacy

73 Privacy and Personal Data Protection Guidelines for Africa, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 2 December 2020).

74 As above.

75 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series, 2020 4.

76 Greenleaf & Cottier (n 75) 5.

77 Sec 2 Constitution.

78 1996 (2) SA 751 (CC)

extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured'. Therefore, the right to privacy is recognised as having two components, namely, that the person must have a subjective expectation of privacy, and that society must have recognised the expectation as objectively reasonable.

Section 32 of the Constitution⁷⁹ in chapter 2 of the Bill of Rights also becomes relevant for the purposes of this chapter. Section 32 reads as follows:

- (1) Everyone has the right of access to –⁸⁰
 - (a) any information held by the state; and⁸¹
 - (b) any information that is held by another person and that is required for the exercise or protection of any rights.⁸²
- (2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.⁸³

In this regard the most relevant provision is section 2 which empowers National Assembly to enact legislation that will give effect to section 32. The essence and relevance of this provision will be discussed later in this chapter. However, the importance of this provision is noted by Ngcobo J in the case of *Brümmer v Minister for Social Development & Others*⁸⁴ in which he affirms the significance of this right, more so in country found on the principles of values of accountability, responsiveness and openness cannot be overlooked.⁸⁵ Peekhaus argues that South Africa is one of the new countries that have made positive progress in enhancing the right to access information.⁸⁶

3.3 Common law

Before the right to privacy was validated by the Constitution, it found its origin from common law. To date the right still enjoys the common law protection as the common law still recognises the right to privacy. A

79 Sec 32 Constitution.

80 Section 32(1) the Constitution.

81 Sec 32(1)(a) Constitution.

82 Sec 32(1)(b) Constitution.

83 Sec 32(2) Constitution.

84 2009 (6) SA 323 (CC).

85 *Brümmer* (n 84) para 63.

86 W Peekhaus 'South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence' (2014) 4 *Journal of Information Policy* 570.

person whose right to privacy has been infringed has recourse in terms of common law to remedy the breach in terms of the *actio iniuriarum*.⁸⁷ If any patrimonial loss is suffered as a result of the infringement of the right to privacy, that person may seek reimbursement in terms of the common law remedy of the *actio legis Aquiliae*. If there is an imminent threat to one's privacy, he or she may apply for an interdict, which is also a common law remedy.⁸⁸ Privacy therefore relates to information, which pertains to an individual who has made a determination that such information to not be revealed to the public. In essence, someone's privacy can be infringed when their facts are made known to the public without their will. Roos submits that this can take two forms. The first is when the outsider took the initiative to learn about the person's facts, which is known as privacy intrusion or acquaintance, or when someone discloses such information to a third party.⁸⁹

3.4 Statutory data protection and privacy

Precisely four known privacy legislations encompass provisions relating to the protection of data and privacy, which are also applicable to social assistance beneficiaries in cases where their data has been illegally used and their privacy has been infringed. Judging from the purpose and nature of these statutes they were enacted to give effect to section 14 of the Constitution, subsequently expanding the protection of data and privacy. The Electronic Communications and Transactions Act 25 of 2002⁹⁰ was intended to regulate electronic communication and also provided for the prevention of the abuse of information.⁹¹ The Act deals with information obtained through electronic transactions and prohibits the data controller from using information without the written permission⁹² of the data subject,⁹³ and it also requires the data controller⁹⁴ to use the data for the purpose for which it was requested.⁹⁵ The Protection of Personal

87 I Currie & J de Waal *The Bill of Rights handbook* (2016) 295.

88 A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *Potchefstroom Electronic Law Journal* 90.

89 As above.

90 Electronic Communications and Transactions Act 25 of 2002.

91 Aim of the Electronic Communications and Transactions Act 25 of 2002.

92 Sec 51(1) ECTA.

93 The ECTA defines the data subject as 'mean[ing] any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act'.

94 The ECTA defines data controller as follows: "'Data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.'

95 Sec 51(2) ECTA.

Information Act 4 of 2013 (POPIA)⁹⁶ is another legislative measure and it is regarded as the primary legislation aimed at promoting the protection of personal information processed by public and private bodies. It goes further in establishing the minimum standards that apply to the processing of information, and its Preamble recognises the significance of the right to privacy as entrenched in section 14 of the Constitution.⁹⁷ POPIA applies to all information processed entered into the record⁹⁸ and requires persons who are in possession of information belonging to someone else to take proactive measures in protecting that information and maintaining confidentiality.⁹⁹ These proactive steps must be put in place to preclude the loss or damage to or even unauthorised access to the personal information concerned.¹⁰⁰

POPIA¹⁰¹ was enacted to give effect to section 32 of the Constitution, therefore ensuring that everyone exercise their right to access information held by the state.¹⁰² The said Act applies to both private and public bodies.¹⁰³ There is a close juxtaposition between the protection of data and access to information. Both these types of rights complement one another because as much the Constitution affords one with the right to access information, it also affords one protection against the infringement of the right to privacy.¹⁰⁴ The Act warrants the information officer to refuse the disclosure of information that belongs to the third if the disclosure can be viewed as unreasonable, or if the person is deceased.¹⁰⁵ POPIA further

96 Protection of Personal Information Act 4 of 2013 (POPIA).

97 Preamble to the Protection of Personal Information Act 4 of 2013.

98 Sec 3 POPIA.

99 Sec 19(1) POPIA.

100 Sec 19(1)(a)-(b) POPIA.

101 POPIA (n 96).

102 Preamble to the Promotion of Access to Information Act 2 of 2002 (PAIA).

103 Sec 3 PAIA.

104 D van der Merwe *Information and communication technology law* (2016) 25.

105 Sec 34 PAIA. Information officer is defined as “‘information officer’ of, or in relation to, a public body (a) in the case of a national department, provincial administration or organisational component (i) mentioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 (Proclamation 103 of 1994), means the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of the said Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or organisational component or the person who is acting as such; or (ii) not so mentioned, means the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or organisational component, respectively, or the person who is acting as such; [sub-para (ii) amended by s 21 of Act 42 of 2001 (wef 7 December 2001).] (b) in the case of a municipality, means the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act 117 of 1998), or the person who is acting as

prohibits the use or disclosure of certain confidential information as well as other related information.¹⁰⁶ POPIA empowers the information officer to decline the disclosure of the information if the information was submitted in confidence by the third party.¹⁰⁷ The legislature has also incorporated provisions that are important for the personal protection of data belonging to grant beneficiaries in the SASSA Act. This evident from section 16 of the SASSA Act which prohibits SASSA from disclosing social grant personal information that was used for purposes of applying for a social grant. However, this is subject to the provisions of the Constitution or POPIA. This clause makes an exception where there is a court order compelling the agency to disclose or where the beneficiary has consented to such.¹⁰⁸

The Agency has done little in a bid to protect social grant beneficiaries' information. Nonetheless, the Constitutional Court is to be commended for compelling the state to put in place adequate safeguard measures to protect beneficiaries' data being illegally used and their privacy right infringed. This may be viewed as an extension of the existing personal protection laws for social grant beneficiaries. Adequate safeguard measures as a means to protect the rights of social grant beneficiaries were stressed out in the *Black Sash* case.¹⁰⁹ The case concerned a middle man called Cash Paymaster Services that was awarded a tender to render social assistance payments for five years, but the tender was found to be constitutionally invalid.¹¹⁰ The Court suspended the declaration of invalidity, based on the premise that either the tender will be awarded fairly after following the proper procurement process, or SASSA will render payments of social grants itself. SASSA decided not to be awarded the tender and to render payment itself. Unfortunately the agency was not able to meet the deadline and no proactive steps were taken by either the agency or the Minister of Social Development to inform the Constitutional Court timeously about its inability to carry out social grant payments.¹¹¹

This case comes after the 2013 judgment, which declared the CPS contract to be invalid and ordered SASSA to conduct a new procurement process or render payments itself. SASSA's failure, together with that of

such; or (c) in the case of any other public body, means the chief executive officer, or equivalent officer, of that public body or the person who is acting as such.'

106 Sec 31 PAIA

107 Section 31(1)(a) PAIA.

108 Sec 16 SASSA Act.

109 *Black Sash Trust* (n 1).

110 *Black Sash Trust* (n 1) para 3.

111 *Black Sash Trust* (n 1) para 6.

the Minister, led to Black Sash reproaching the Court on the basis of the state's non-compliance with the 2013 court order. Chief among the orders that were made by the Court was that personal information that belonged to the beneficiaries should remain with SASSA and only be utilised for social grants payments.¹¹² The Black Sash Trust applied for direct access on an urgent basis. Black Sash further sought for the following orders:

- (a) that SASSA must file a report on affidavit on how it intends to deal with an interim contract with CPS for payment of social grants from 1 April 2017;
- (b) declaring that CPS is under a duty to act reasonably in negotiating that contract with SASSA;
- (c) that the contract must contain adequate safeguards for various aspects of the personal privacy, dignity and autonomy of grant beneficiaries;
- (d) that the Minister and SASSA must file continuous reports with the Court on the steps taken and to be taken to ensure that payment of social grants is made from 1 April 2017; and
- (e) declaring that SASSA is under a duty to ensure that the payment method must contain adequate safeguards for various aspects of the personal privacy, dignity and autonomy of grant beneficiaries.¹¹³

In light of the above prayers of the applicant, the Court granted the application for direct access, Freedom Under Law was granted leave to intervene and Corruption Watch and the South African Post Office were admitted as friends of the court. The Court further declared that SASSA was under a constitutional obligation to make social grants payments; the suspension on the invalidity of the CPS contract was extended; and CPS as well as SASSA were required to ensure that payment of social assistance grants was effected. The contract was to remain intact and invariable. The Court furthermore ordered that the contract contains provisions that will outline safeguard measures that will enable the safety of personal data of beneficiaries so that it is used for payment purposes only. It was further held that the contract also contains a provision that will prevent inviting beneficiaries in opt-in opt-out or disclose their information for marketing purposes, which was also declared as SASSA's duty to do so.

This case seems to have paved the way for the state's duty, in particular that of SASSA, to ensure that safety measures are put in place that protect data belonging to social grant recipients and prohibit the invasion of their privacy. The case still finds expression and relevancy even in today's social

112 *AllPay Consolidated Investment Holdings (Pty) Ltd v Chief Executive Officer, South African Social Security Agency* ZACC 42; 2014 (1) SA 604 (CC).

113 *Black Sash Trust* (n 1) para 23.

assistance set-up, alongside with the provisions of POPIA and any other relevant statute that may be used in protecting social assistance beneficiaries. It is worth mentioning that POPIA is the most preferred legal avenue to explore in cases of privacy breach of social assistance beneficiaries. This is not to disregard the existing laws that directly or indirectly feed up to the purpose and intention of section 14 of the Constitution.¹¹⁴ However, POPIA¹¹⁵ displays the shortcomings in the existing legislations including the SASSA Act¹¹⁶ and the SAA.¹¹⁷

The provisions relating to data protection and the right to privacy are made enforceable through the Information Regulator, an institution established in terms of section 39 of POPIA.¹¹⁸ The Information Regulator has jurisdiction across the country;¹¹⁹ it is impartial¹²⁰ and is required to function in accordance with the Constitution, POPIA,¹²¹ and is accountable to the legislature.¹²² The Regulator is entrusted with the role of monitoring compliance with the Act by both the private and public sectors; this therefore means that the Act is applicable to SASSA and contracted companies.

4 Challenges

There is no doubt that there has been impactful progress in the South African social assistance arena, with two fundamental legislations being promulgated to regulate the social assistance industry, namely, the Social Assistance Act¹²³ and South African Social Security Agency Act.¹²⁴ These developments necessitated the amelioration of the social assistance system in terms of the digitisation and social grant payments. This is evident in the year 2012 when SASSA introduced electronic payments via the SASSA MasterCard, which initiative was intended to reduce fraud and the possible cost of disbursement.¹²⁵ With the evolving technology

114 Sec 14 Constitution.

115 POPIA (n 96).

116 SASSA Act.

117 Social Assistance Act.

118 Sec 39 POPIA.

119 Sec 39(a) POPIA.

120 Sec 39(b) POPIA.

121 Sec 39(c) POPIA.

122 Sec 39(d) POPIA.

123 Social Assistance Act.

124 South African Social Security Agency Act.

125 AB Fanta and others 'Digitisation of social grant payments and financial inclusion of grant recipients in South Africa – Evidence from FinScope surveys' (2017) *Social Security Review* 2.

across the country and SASSA being no exception to this, there was a dire need for new laws and the amendment of the existing laws so as to protect possible victims against cybercrimes or fraud. Hence, the enactment of the above statutes such as POPIA, ECTA and the SASSA Act as well as the landmark case of *Black Sash*, which enunciated the need for SASSA to implement safety measures that will enable data protection and privacy when contracting with third parties to render payment services to recipients of social assistance grants.

Notwithstanding some of the highlighted developments that have thus far taken place, there are still some glaring challenges faced by SASSA, ultimately affecting social grants beneficiaries, and what is even detrimental is that social assistance beneficiaries are vulnerable people. The first challenge is beneficiaries' information, which still in the possession of Net1 that refuses to return the information.¹²⁶ These allegations were brought forward by Black Sash when it was called upon to make submissions at the United Nations General Assembly on digital technology, social protection and human rights. Furthermore, Net1 has been linked with a company called EasyPay Everywhere, which has low bank charges and has recruited largely social grants beneficiaries, raising concerns after Net1 refused to submit information at its disposal, which might have been used in this process.¹²⁷ This occurred despite the standing order of the Constitutional Court, which states:

The terms and conditions shall:

- (a) contain adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004; and
- (b) preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹²⁸

This is also in contravention of section 3(c) read with section 16 of the SASSA Act which states that no person may dispose of social grant beneficiary information, unless there is a court order compelling one to

126 Black Sash submission at United Nations General Assembly on Digital Technology, Social Protection and Human Rights in May 2019 9.

127 <https://www.news24.com/fin24/Economy/did-cps-lie-about-its-social-grant-profits-20171119-2> (accessed 20 September 2020).

128 *Black Sash Trust* (n1) para 76.

do so.¹²⁹ Prinsloo contends that SASSA does not have a well-equipped information technology (IT) infrastructure, also imparting data belonging to SASSA beneficiaries to cybercrime syndicates. This effectively means that SASSA is in dire need of an improved IT infrastructure that will not only be beneficial to the agency only but to social grant beneficiaries. Sending misleading information through SMSs to these beneficiaries is said to be an indication of a poor IT infrastructure; staff members are alleged to have sold beneficiaries' confidential information.¹³⁰

The above continued illegal use of data and the infringement of the right to privacy also contravene the provisions of POPIA. The Act is the primary legislation, which was enacted to give rise to section 14 of the Constitution¹³¹ and the principal legislation dealing with data protection and privacy. POPIA is described as serving its envisaged purpose within the data protection spectrum, which is evident through the provision it made pertaining to the development of a comprehensive legal framework.¹³² The Act comprises a chapter dealing with conditions of lawful processing of personal information¹³³ which, among other provisions, provides that information should be collected for a legal purpose¹³⁴ and requires that the concerned party be made aware when collecting information.¹³⁵ The said chapter further contains a crucial provision, which demonstrates proactive steps to be taken as security measures on integrity and confidentiality of personal information.¹³⁶ The responsible party is required to maintain confidentiality and integrity of personal information at its disposal. This is to be done by taking technical, appropriate, reasonable and organisational steps.¹³⁷ This will prevent the 'loss of or damage to or unauthorised destruction of personal information¹³⁸ and unlawful access to or processing of personal information'.¹³⁹ To archive

129 Sec 3(c) read with sec 16 SASSA Act.

130 T Prinsloo & S Ntondini 'The exploitation of South African Social Security Agency grant recipients' data' Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development 2018.

131 Sec 14 Constitution.

132 A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments' (2016) 79 *Journal for Contemporary Roman-Dutch Law* 16.

133 Ch 3 POPIA.

134 Sec 13(1) POPIA.

135 Sec 18(1) POPIA.

136 Sec 19 POPIA.

137 Sec 19(1) POPIA.

138 Sec 19(1)(a) POPIA.

139 Sec 19(1)(b) POPIA.

this, the responsible party must take proactive measures that will assist in foreseeing internal and external risks that may be posed to the personal information of the data subject.¹⁴⁰ The responsible party should develop safeguard measures to fulfil this purpose.¹⁴¹ The Act requires responsible parties to continuously do quality checks of the safety system measures to establish whether or not they are still effective.¹⁴² There is no doubt that SASSA's safety net measures have been tampered with on numerous occasions. Thus, they have been rendered ineffective, effectively meaning that SASSA has failed to keep up with its system to enable an effective system that safeguards personal information. To keep abreast with new risks, safeguards need to be regularly updated,¹⁴³ which will allow SASSA to counteract efforts of cybercrime syndicates that explore new ways of accessing grant beneficiaries' personal information and, subsequently, the illegal use of their data and infringing their right to privacy.

Batchelor and Wazvaremhaka note financial illiteracy as another contributing factor relating to the recent invasion of data and privacy. Unfortunately, financial service providers have taken advantage of the fact that most social assistance beneficiaries are illiterate and, as a result hereof, some were exposed to financial discrepancies.¹⁴⁴ Therefore, financial education for social assistance beneficiaries is paramount, which will enable them to better understand how to manage finances. Dutschke reminds us of the primary existence of SASSA, namely, that it was established in order to deal with the poor administration of social grants that existed at the time and this adversely affected the receipt of social grants. The Agency was necessitated by the delay in social grant payments, which was monitored at provincial level, and the establishment of the Agency meant that the responsibility to administer social grant payments will now be transferred to the national level.¹⁴⁵ This was also made possible by the Constitutional Court in the case of *Mashavha v President of the Republic of South Africa* when it declared the administration of social grants to be invalid and unconstitutional but suspended the invalidity.¹⁴⁶

140 Sec 19(2)(a) POPIA.

141 Sec 19(2)(c) POPIA.

142 Sec 19(2)(d) POPIA.

143 Sec 19(2)(d) POPIA.

144 Batchelor and Wazvaremhaka (n 21) 14-15.

145 M Dutschke 'Improving the administration of social assistance services' (2008) 9 *Economic and Social Rights in South Africa* 12.

146 2004 ZACC 6; 2005 (2) SA 476 (CC).

Another factor to be considered that contributes to the illegal use of data and breach of privacy that belongs to social assistance payments is the poor administration at SASSA. There are numerous challenges that affect SASSA to operate optimally. In this chapter all these challenges that have a bearing on the protection of data and privacy that emanate from the Agency are summed up under the term 'poor administration'. For the purposes of this chapter, poor administration includes the delays in payments that are associated with slow capturing, verification and approval, which sometimes is attributed to the fact of shortage of human resources. The absence of technological infrastructure also adds no value in the purpose of archiving effectiveness in the social assistance system.¹⁴⁷ Therefore, it is worth noting from the latter on SASSA's administration that the Agency is grappling with maladministration, which cannot be separated from the shortcomings on data protection and privacy faced by social assistance beneficiaries. In the case of *Cele v The South African Social Security Agency and 22 related cases* the Court expressed its concern over the blockages of applications of social assistance that are occasioned by incompetent officials, poor administration and numerous legal battles.¹⁴⁸

The lack of effective legal measures to protect data and curb efforts to infringe the right to privacy has also been associated with high levels of grant corruption within the Agency. This is evident from the annual report released by the Public Service Commission (PSC), which revealed social grants corruption as the highest corruption, at 2 400 cases between the financial years 2017/2018-2020/2021. Social grant fraud is one of the most reported fraud cases on the national anti-corruption hotline NACH. It is said that most social grant cases are occasioned 'identified along with unethical behaviour, appointment irregularities, service delivery and procurement irregularities'.¹⁴⁹ In the past, due to the high levels of corruption and fraud in social assistance, which included fake identity of receipts and fraudulent claims, this enunciated on SASSA to develop biometrics in a bid to assist in identification and eliminate fraud.¹⁵⁰ SASSA not only is in contravention of POPIA or the SASSA Act by not having effective legal measures, but also contravenes the Social Protection Floors Recommendation 202 of 2012¹⁵¹ as it requires member states to set up

147 http://repository.nwu.ac.za/bitstream/handle/10394/9515/Joseph_DE_Chapter_4.pdf?sequence=5 (accessed 30 October 2022).

148 2008 (7) BCLR 734.

149 <https://citizen.co.za/news/south-africa/investigation/2358392/social-grant-fraud-records-highest-number-of-alleged-corruption-cases-psc-report/> (accessed 2 October 2020).

150 As above.

151 Social Protection Floors Recommendation 202 of 2012.

effective social security systems with proactive steps to protect the data of social grant beneficiaries.¹⁵²

5 Recommendations

With respect to the looming social grants discrepancies, the need to establish the Social Assistance Inspectorate is necessary and urgent as ingrained in chapter 4, section 24 of the Social Assistance Act.¹⁵³ This will enable the inspectorate to effectively investigate and deal with complaints around grant corruption, fraud, the illegal use of data, the infringement of privacy as well as cybercrime of which social grants beneficiaries are victims.

The Social Assistance Act makes provision for the establishment of an inspectorate for social assistance. An executive director must be appointed to head the inspectorate,¹⁵⁴ which will function independently from SASSA and the Department of Social Development.¹⁵⁵ The rationale behind this provision is to ensure the independence of this institution. I hold a different view from the legislature on this aspect, because the envisaged independence of the inspectorate will be impaired and tempted as the Act permits the minister to exercise full responsibility over the inspectorate. In some instances, complaints from social grants beneficiaries may be extended to the minister who can necessitate the inspectorate to also investigate the ministry. The final outcome may be compromised by possible interference, which also affect the credibility of the inspectorate report.

The inspectorate is tasked with maintaining the frameworks and systems of social assistance.¹⁵⁶ It was also tasked to perform internal audits and monitor compliance with the Agency's policy and relevant laws.¹⁵⁷ The inspectorate was also meant to investigate fraud, corruption and mismanagement as well as criminal activities.¹⁵⁸ Since the enactment of the Social Assistance Act, the inception of the inspectorate remains a dream that is not yet realised. South Africa should derive certain lessons from the United States as far as an independent inspectorate is concerned. In the US there has been the establishment of the Office of the Inspector

152 Para 23 Social Protection Floors Recommendation (n 151).

153 Ch 4, sec 24 Social Assistance Act.

154 Sec 24(1) Social Assistance Act.

155 Sec 24(1) Social Assistance Act.

156 Sec 27(1)(a) Social Assistance Act.

157 Sec 27(1)(b) Social Assistance Act.

158 Sec 27(1)(c) Social Assistance Act.

General (OIG).¹⁵⁹ The establishment of the OIG finds expression in the Social Security Independence and Programme Improvements Act¹⁶⁰ and its authority generally emanates from Inspector General Act of 1978.¹⁶¹ The responsibility of the office is to protect social security integrity. The OIG monitors the activities of the management to ensure effectiveness and ensures that it curbs fraud within the social security administration. The inspectorate has been reported to be effective and has assisted in ensuring efficiency as well as eliminating conduct of fraud within social security administration.¹⁶²

Although smart cards were introduced to ensure efficiency with regard to social assistance payments and eliminate possible fraud activities, some obscurities remain as the current method of payment only requires the cardholder or beneficiary to punch in the pin after presenting the card. This can practically mean that anyone can get a hold of the pin and present themselves as the card owner at any pay point or ATM. To curb this detrimental form of payment, card payments that include biometrics payment is hereby proposed.¹⁶³ This method requires a sensor/finger print reader on the card before presenting the card so as to ensure that the individual really is the card holder. Therefore, before the use of the card, the beneficiary will activate their card by using a finger, which will ensure that the card is only used by the owner who is the beneficiary to curb acts of fraud.¹⁶⁴

As highlighted earlier, Net1 and its subsidiaries still possess personal information of social grant beneficiaries, which they use to advertise their products, and they eventually use the data without consent, also infringing their right to privacy. The Constitutional Court judgment in the *Black Sash* case¹⁶⁵ has attempted to curb such malpractice despite the fact that there is no compliance. The Court held that SASSA and CPS must ensure that the following terms and conditions are imbedded in the contract:

159 Social Security Administration (SSA), Office of Inspector General (OIG) Special Agent Handbook, 2002, https://www.governmentattic.org/27docs/SSAoigSpecAgentHdbk_2002.pdf (accessed 27 November 2020).

160 Social Security Independence and Programme Improvements Act of 1994.

161 Inspector-General Act of 1978.

162 Social Security Administration (SSA), Office of Inspector General (OIG) Special Agent Handbook, 2002, https://www.governmentattic.org/27docs/SSAoigSpecAgentHdbk_2002.pdf (accessed 27 November 2020).

163 S Mthethwa & M Thiyanne 'An improved smartcard for the South African Social Security Agency (SASSA)' 3rd International Conference on Information Science and Security, Pattaya, Thailand, 2020 3.

164 As above.

165 *Black Sash Trust* (n 1) para 1.

- (a) contain adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister in terms of section 20(3) and (4) of the Social Assistance Act 13 of 2004;¹⁶⁶ and
- (b) preclude anyone from inviting beneficiaries to 'opt-in' to the sharing of confidential information for the marketing of goods and services.¹⁶⁷

Therefore, the state needs to ensure that there is compliance with the Constitutional Court judgment, and Net1 should return the grant beneficiaries' personal information to SASSA as the chief custodian of personal information of social grant beneficiaries. In the case of failure or refusal by Net1 to hand over the personal information belonging to grant beneficiaries, the state should lodge an application of contempt of court. To further compel Net1 to comply with the provisions of the Constitutional Court judgment and to ensure that the state execute the order effectively and efficiently, one needs to build a substantive argument through the lenses of the ongoing discourse of judicial enforcement of socio-economic rights. The enforcement of socio-economic rights has come under close scrutiny in two famous Constitutional Court cases, namely, the *Grootboom* and *Soobramoney* cases. The significance of these cases on this aspect was thus amplified in the *TAC v Minister of Health* case wherein it reiterated that the state is under a constitutional obligation to comply with or fulfil the obligations imposed by sections 26 and 27 of the Constitution.¹⁶⁸ De Beer and Vettori submit that over the past years the judiciary has been rather creative and cautious in treating matters relating of socio-economic rights with the urgency they deserve. The non-compliance by state officials and other personnel may be regarded as a high level of ignorance and arrogance about their duties as well as the powers of courts of law in this regard. They further submit various modes of enforcing and ensuring compliance with judgments on socio-economic rights such as structural interdicts, contempt of court, as mentioned earlier, and delictual damages.¹⁶⁹

The judicial enforcement of socio-economic rights cannot be overemphasised but rather demonstrates the causal nexus between the said enforcement and data protection and privacy. If there is no adequate protection afforded to social grant beneficiaries in terms of their personal

166 *Black Sash Trust* (n 1) paras 76, 6.1(a).

167 *Black Sash Trust* (n 1) paras 76, 6.1(b).

168 *TAC v Minister of Health* para 23.

169 RJ de Beer & S Vettori 'The enforcement of socio-economic rights' (2007) 10 *Potchefstroom Electronic Journal* 26.

data and privacy rights, this eventually impairs their right to social assistance, which is categorised under the umbrella of socio-economic rights. On account of the latter fraud, corruption and cybercrimes are perpetuated as a result of the state's failure to honour the Constitutional Court judgment, with appalling consequences for the needy and vulnerable social grant beneficiaries. Hence, I concur with De Beer and Vettori on the alternatives they have explored, namely, should the state fail or refuse to execute the judgment, which include structural interdicts, contempt of court and delictual damages.

POPIA¹⁷⁰ gave rise to the establishment of the Information Regulator, which functions in accordance with this Act¹⁷¹ and Promotion of Access to Information Act.¹⁷² The Information Regulator is accountable to the National Assembly.¹⁷³ The state together with SASSA should make use of the Regulator as an enforcement agency in cases of illegal use of data and invasion of the right to privacy. While there is no hope of commitment by the state to establish the social assistance inspectorate, SASSA can in the meantime partner with the Regulator in eliminating all forms of illegal use of data belonging to grant beneficiaries that impairs their right to privacy. Among the duties, powers and functions of the Regulator, the Regulator promotes the lawful processing of personal information¹⁷⁴ and also oversees both private and public institutions' compliance with the provisions of POPIA.¹⁷⁵ Furthermore, the Regulator has the power to receive and investigate complaints pertaining to the misuse of personal information.¹⁷⁶ With such provisions of POPIA that empower the Regulator to decisively deal with acts of impropriation of data and invasion of privacy, SASSA may consider the Regulator a better institution to protect data and privacy rights of grant beneficiaries.

Since the introduction of technological changes in the Agency, there has been resistance from workers, evidenced by the workers' protest led by National Education Health and Allied Workers Union (NEHAWU). Top on the list of demands was that biometric enrolment was impractical given the fact that most SASSA branches are less equipped and most staff are not technologically capacitated, and that they would need to undergo

170 POPIA (n 96).

171 Sec 39(c) POPIA.

172 Promotion of Access to Information Act 2 of 2000.

173 Sec 39(d) POPIA.

174 Sec 40(1)(a)(i) POPIA.

175 Sec 40(1)(b)(i) POPIA.

176 Sec 40(1)(d)(i) POPIA.

training before enrolment.¹⁷⁷ Hence, it is recommended that it would be prudent for the Agency to arrange continued training to enable workers be familiar with the advanced system. This will also ensure the proper running of the Agency without any hiccups relating to maladministration.

Many grant beneficiaries are vulnerable and illiterate people who lack financial capabilities, as highlighted earlier on. SASSA should also focus more on financial education of these social grant beneficiaries to improve their financial capabilities and better handling of their finances. The South African Grant Distribution report highlights some meaningful impacts on these people if financial education is conducted. These factors are the following:

- increase grant recipients' household and personal ability to achieve their medium and long-term financial goals;
- increase their household and personal overall welfare;
- enable grant recipients to build on their increased resilience;
- support the most vulnerable segments to be able to cope with hardships, and avoid falling into food insecurity or deep and sustained misery;
- improve the financial sector's ability to cater for the needs of low-income segments of the market;
- foster South Africa's economic growth;
- ensure that the nation's budget can become more sustainable and ensure that public expenditures are affordable for the nation, thus reducing the debt burden on the economy.¹⁷⁸

6 Conclusion

Social assistance programmes that have been implemented over the past years are evidence that the state is committed to archiving socio-economic rights, because social assistance programmes are based solely on government's revenue in order to effect social grant payments to the needy. Due to the technological advancements in the area of social grants through SASSA, it has thus necessitated the enactment of legal measures to prevent the beneficiaries from being exposed to crimes by and conduct of cyber syndicates. It is against this background that a legislative framework was enacted, but most importantly to give rise to section 14 of the Constitution.

177 <https://www.timeslive.co.za/news/south-africa/2018-10-10-sassa-workers-go-on-strike> (accessed 12 December 2020).

178 South Africa SASSA Grant Distribution Improving the financial capability of grant recipients report, https://www.finmark.org.za/system/documents/files/000/000/276/original/SASSA_Grant_Recipients_-_Improving_the_Financial_Capability.pdf?1605614633 (accessed 15 December 2020).

Social assistance beneficiaries are entitled to social assistance programmes should they be unable to support themselves, as entrenched in section 27 of the Constitution.¹⁷⁹ All that is required from them is to submit their documents with their personal details to the processing officer who later processes the application and the applicant will be informed of the outcome of the application. During this period and even afterwards, the applicants enjoy constitutional protection of their personal information through section 14 of the Constitution.¹⁸⁰ With these constitutional rights bestowed on social grant beneficiaries, the state is constitutionally obliged to respect, protect, promote and fulfil the rights in the Bill of Rights.¹⁸¹ Not only do grant beneficiaries enjoy constitutional protection but legislative protection as well through the lens of section 16 of the SASSA Act,¹⁸² which prohibits anyone from disposing of any information relating to the social grant beneficiaries subject to the provisions of the Constitution, POPIA¹⁸³ or a court order.¹⁸⁴

Therefore, the *Black Sash* case paved the way forward to enable the state to effectively protect social grant beneficiaries' data from illegal use and to avoid the infringement of their rights to privacy. Safeguard measures should be a priority for the state when processing social grant applications. Even after the application process the state is under an obligation to safeguard personal information belonging to social grant beneficiaries.

179 Sec 27 Constitution.

180 Sec 14 Constitution.

181 Sec 7 Constitution.

182 Sec 14 Constitution.

183 POPIA (n 96).

184 Sec 16(1) SASSA Act.

References

- Batchelor, B & Wazvaremhaka, T 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development* 2017 (9) 1089 (CC)' (2019) 136 *South African Law Journal* 129
- Currie, I & De Waal, J *The Bill of Rights handbook* (2016)
- De Beer, RJ & Vettori, S 'The enforcement of socio-economic rights' (2007) *Potchefstroom Electronic Law Journal* 26
- Dutschke, M 'Improving the administration of social assistance services' (2008) 9 *Economic and Social Rights in South Africa* 12
- Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments (2020) 4, <https://citizen.co.za/news/south-africa/investigation/2358392/social-grant-fraud-records-highest-number-of-alleged-corruption-cases-psc-report/> (accessed 2 October 2020)
- Mthethwa, S & Thiyanne, M 'An improved smartcard for the South African Social Security Agency (SASSA)' 2020, 3rd International Conference on Information Science and Security, Pattaya, Thailand 3
- Naude, A & Papadopoulos, S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments' (2016) 79 *Journal for Contemporary Roman-Dutch Law* 16
- Orji, UJ *The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?* (2018)
- Peekhaus, W 'South Africa's Promotion of Access to Information Act: An analysis of relevant jurisprudence' (2014) 4 *Journal of Information Policy* 570
- Prinsloo, T & Ntondini, S 'The exploitation of South African Social Security Agency grant recipients' data' (2006) *International Journal of Social Welfare* 16
- Roos, A 'Core principles of data protection law' (2006) 39 *Comparative and International Law Journal of Southern Africa* 103
- Roos, A 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 11 *Potchefstroom Electronic Law Journal* 90
- Van der Merwe, D *Information and communication technology law* (2016)

PART IV: Data privacy during the COVID-19 pandemic

9

TRACKING COVID-19: WHAT ARE THE IMPLICATIONS FOR DATA PRIVACY IN AFRICA?

*Alex Boniface Makulilo, Rindstone Bilabamu Ezekiel,
Doreen Mwamlangala and Mbiki Msumi*

Abstract

The outbreak of COVID-19 and its spread into a pandemic have compelled governments worldwide to take stern measures to protect their populations. As elsewhere, different African governments are tracking, tracing, collecting and using personal data to slow down the spread of COVID-19. Many African countries use physical contact tracing in which individuals that tested positive are interviewed to identify locations where they had been and identify people whom they had met. Some few countries have started using tracking applications so as to complement physical tracking methods and, hence, provide additional data sources. Notwithstanding the necessity of protecting the health of residents from the pandemic, the fact that this protection hinges on sensitive personal data of individuals raises concerns for data privacy in Africa. This chapter offers a detailed discussion of the implications for the privacy of tracking applications in the context of COVID-19 in Africa. Examples will be taken from different African jurisdictions. Specifically, the chapter answers the question of whether data privacy laws in Africa are capable of protecting personal data in the context of COVID-19.

1 Introduction

The outbreak of the corona virus pandemic was reported for the first time in late 2019 in Wuhan, Hubei province, China. It rapidly became a worldwide threat as it raised health concerns and has continued to pose a threat to people's lives.¹ The virus threat in China drew the attention of the Chinese Centre for Disease Control,² leading to the isolation of a new corona virus, COVID-19. This novel virus has persistently caused thousands of deaths globally. Only in January 2020, the outbreak rapidly engulfed the countries of China, Thailand, Japan, South Korea, Singapore, Vietnam, Taiwan, Nepal and the United States. At different stages, the world witnessed the spread of COVID-19 between late-January and mid-

1 Coronaviruses have been described as single, plus-stranded RNA viruses belonging to the family *Coronaviridae* including MERS (MERS-CoV) and SARS (SARS-CoV).

2 H Lu and others 'Outbreak of pneumonia of unknown etiology in Wuhan, China: The mystery and the miracle' (2020) 92 *Journal of Medical Virology* 401-402

February 2020 from Hubei province, China to Northern Italy; from China to Washington state; and, later, from Europe to New York City and from China to California.³ Although many details of the emergence of this virus have remained controversial, the COVID-19 pandemic continued to surge and, in Africa, with severe health, social, and economic impacts on an unprecedented scale.

In Africa, the first confirmed cases of COVID-19 were reported in Egypt,⁴ South Africa,⁵ Senegal,⁶ the Democratic Republic of the Congo (DRC),⁷ Nigeria, Algeria and several other African countries. Available data reveals that apparently all early cases were imported in Africa among travellers from Europe. Subsequently, the majority of COVID-19 cases that were identified and reported in many African countries were the result of local transmission.

The pandemic has significantly affected people's lives and livelihoods due to upheavals of the pandemic that has claimed and continues to claim thousands of lives in many countries. Almost every country that was hit hard by COVID-19 had its health systems overwhelmed. Without any alternatives for livelihood, many countries shut down markets, airports, hotels, sports and public transport.

In an attempt to contain the rapid spread of the pandemic, many countries around the world introduced a range of measures underpinning

- 3 D Stole 'How Coronavirus took hold in North America and Europe, Igniting Major COVID-19 Outbreaks' <https://scitechdaily.com/how-coronavirus-took-hold-in-north-america-and-europe-igniting-major-COVID-19-outbreaks/> (accessed 12 September 2020).
- 4 On 14 February 2020.
- 5 On 29 February 2020. A group of nine adult travellers returned from a skiing holiday in Italy, where the COVID-19 epidemic was rampant. After developing a flu-like illness, one traveller tested positive for COVID-19, which was confirmed by RT-PCR on 5 March 2020; his wife was asymptomatic but tested positive on 8 March 2020. Overall, seven of the nine travellers tested positive for COVID-19, five of whom were asymptomatic.
- 6 World Health Organization, African Region 'Senegal reports first COVID-19 case' <https://www.afro.who.int/news/senegal-reports-first-COVID-19-case> (accessed 12 April 2020). In Senegal, the first COVID-19 case was reported on 7 March 2020 whereby a traveller returning from Italy led to contact tracing that identified a cluster of transmission of 20 cases within his immediate household.
- 7 World Health Organization 'First Case of COVID-19 confirmed in Democratic Republic of the Congo' <https://www.afro.who.int/news/first-case-COVID-19-confirmed-democratic-republic-congo> (accessed 20 January 2021). DRC Congo confirmed its first case of COVID-19 on 10 March 2020 which involved an adult male who tested positive in the capital city of Kinshasa after developing a cough and fever, two days after returning from France.

key guiding responses to the spread of the pandemic. These included measures recommended by the World Health Organisation (WHO) and additional measures preferred by individual countries. These include quarantine whereby a person or group of people who have been exposed to a contagious disease were separated even if they had not become sick. This trend has been variably implemented by countries and continues to be imposed in some countries around the world. This has been believed to be capable of preventing the possible spread of COVID-19. Lockdown restrictions were introduced by many countries in response to the spread of COVID-19 across the European region, Asia, North and South America as well as, to a certain extent, in Africa. Other measures include regular hand washing with soap and water; coughing into a tissue or a bent elbow, ensuring to afterwards safely dispose of the tissue; maintaining a social distance of at least one to two metres, particularly if a person is coughing; avoiding touching the eyes, nose and mouth; and seeking early medical attention if a person develops a fever or cough.

Some countries have continued to invest in low-cost preventive measures to improve physical distancing, namely, stopping international travel, reducing the number of people at religious and social gatherings, and universal masking using non-medical cloth masks for the community. Other measures could focus on protecting older people, allowing individuals restricted working hours for income generation, information campaigns for personal hygiene, physical distancing, and hand washing. As lockdowns and physical distancing measures are eased, proactive surveillance, case detection, and contact tracing with isolation will be required to prevent a dramatic resurgence of COVID-19 cases. African health ministries are working closely with African Ministries of Health, Africa CDC alongside the WHO in preventive measures to curb the spread of COVID-19. Individual countries have gone further to develop mechanisms for use of technologies in contact tracing.

2 COVID-19 contact tracing and modern technology

Contact tracing is an essential public health measure and a critical component of comprehensive strategies to control the spread of COVID-19. Contact tracing breaks the chains of human-to-human transmission by identifying people exposed to confirmed cases, quarantining them, following up with them to ensure rapid isolation, and testing and treatment in case they develop symptoms⁸. When systematically and effectively implemented,

8 World Health Organization 'Contact tracing and quarantine in the context of COVID-19: Interim Guidance' 6 July 2022 <https://www.who.int/publications/i/>

these actions can ensure that the number of new cases generated by each confirmed case is maintained below one. In the context of COVID-19, contact tracing requires identifying persons who may have been exposed to a person with COVID-19 and following them up daily for 14 days from the last point of exposure. Since COVID-19 transmission can occur before symptoms develop, contacts should remain in self-quarantine during the 14-day monitoring period to limit the possibility of exposing other people to infection should they become ill.⁹

In response to the COVID-19 pandemic, many digital tools have been developed to assist with contact tracing and case identification. These tools include outbreak response, proximity tracing, and symptom tracking tools, which can be combined into one instrument or used as stand-alone tools.¹⁰

Africa has been less affected than Europe by the corona virus crisis, but the number of cases is increasing as the pandemic progresses across the continent. Many African countries have been severely hurt by the corona virus pandemic. In Africa, COVID-19 is disrupting millions of lives. Poor people and small and informal businesses are having particular difficulties getting by. Even with containment measures such as lockdowns and quarantines, the pace of this disruption is likely to accelerate in the months ahead.

South Africa is still in its infancy stages in developing mobile application technologies to be used as part of the contact tracing process. The South African government together with the University of Cape Town recently developed a mobile application called Covi-ID. The use of the application is by voluntary consent and as yet there are no state-mandated mobile application that people are expected to download and use. Similarly, the government operates a WhatsApp platform that provides people with information on the corona virus as well as information on symptoms of COVID-19. The WhatsApp platform has been criticised for a lack of transparency on the terms and conditions available regarding the processing of personal information collected via the platform.¹¹

item/WHO-2019-nCoV-Contact_tracing_and_quarantine-2022 (accessed 6 July 2022).

9 As above

10 K Servick 'COVID-19 contact tracing apps are coming to a pone near you. How will we know whether they work?' <https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how> (accessed 2 January 2021).

11 Y Jacobs 'SA launches free Covid-19 contact tracing app: This is how it works' <https://www.iol.co.za/technology/mobile/sa-launches-free-COVID-19-contact-tracing-app->

On the other hand, Ghana launched a new application called the COVID-19 Tracker Application that is designed to help in tracing people who have come into contact with COVID-19-positive individuals. The application is meant to augment the government's effort in the fight against the virus.¹² The application is able to trace contacts of persons infected by the virus and show where they have been in recent times through various telephone-related data, and link such people to health professionals for urgent action to be taken.¹³ The application, through the same telephone-related data, is also able to report contacts that are, or recently have been to COVID-19-hit countries, as well as track whether individuals required to self-quarantine indeed are doing so.

However, the implementation of this application has also raised public concerns over the security of personal information required by the application to help in identifying and tracing persons who have come into contact with infected persons.¹⁴

In similar vein, on 23 March 2020 Kenya launched an application for contact tracing. Public service vehicle operators and passengers are required to provide information that helps trace the movements of people who have contracted the corona virus. All public drivers or operators are required to enrol using their vehicle registration numbers and collect details of every passenger. The application is expected to trace all the contacts made by an infected person inside public vehicles. An estimated 50 per cent of the Kenyan population daily uses public transport.¹⁵

On the other hand, technology developers in Kenya have introduced a contact tracing application by the name of KoviTrace¹⁶ to help authorities trace the movement of patients who have tested positive for COVID-19, as well as those who have come into contact with these patients. The application can be installed on Android and IOS¹⁷ phones or accessed

this-is-how-it-works--24b27e8b-d30f-43e4-82a5-4d508255c5cb (accessed 2 January 2021).

12 ITUNews 'Ghana launches COVID-19 Tracker App' <https://news.itu.int/ghana-launches-COVID-19-tracker-app/> (accessed 2 January 2021).

13 As above.

14 'Ghana launches GHcovid19 symptom tracker to contain the spread of COVID-19' <https://furtherafrica.com/2020/05/14/ghana-launches-ghCOVID19-symptom-tracker-to-contain-the-spread-of-COVID-19/> (accessed 2 January 2021).

15 European Investment Bank (EIB) 'Africa's digital solutions to tackle COVID-19' https://www.eib.org/attachments/country/africa_s_digital_solutions_to_tackle_COVID_19_en.pdf (accessed 12 September 2020).

16 This is a diagnostic test for the detection of Sars-cov-2 virus in nasal swab and saliva.

17 iPhone Operating System. This functions only on Apple iPhone, iPod, iPad, iWatch, Apple TV and iMac.

through unstructured supplementary service data (USSD) for users without smart phones.¹⁸ It uses geo-sensing technology to track a patient's location at any given time over a 14-day period from the precise moment they tested positive.¹⁹ The user will need to key in the patient's phone number and command it to trace all the persons with whom the patient came into contact within the stipulated time period. Currently authorities and health officials are relying on patients themselves to remember who they have been in contact with for the past 14 days.

Rwanda has deployed digital tools in contact tracing for coronavirus infections, following in the steps of several countries that are using smart phone data and other digital surveillance tools to curb the virus from spreading further.²⁰ Aware that it is difficult to fully rely on the information provided by those who tested positive, Rwanda opted for a digitised contact tracing method.²¹

The team then tracks other phones that came in close contact with the infected person's phone using movement analytics. Deeper data analysis is then carried out and information obtained helps the COVID-19 command centre to trace these people and contact them for testing. The method has so far proved effective: Reports show this, as most of those who tested positive and those they with whom they got in contact had smart phones. Besides contact tracing, information technology (IT) solutions are also used to monitor and geo-fence people in localised isolation centres to keep them in areas of confinement while data obtained help to inform law enforcement agencies of people violating social distancing rules in areas of concentration.²²

In Nigeria mobile applications and web platforms have emerged as some of the prevailing tools to educate, test and track people to curb the virus from becoming more disastrous than it already is. As of 9 June 2020 the total number of confirmed COVID-19 cases in Nigeria had risen to over 12 000 with 361 deaths.²³ As of 23 February 2021 Morocco accounted for around 8,4 per cent of the casualties on the African continent. Egypt was the second most affected on the continent, as the virus affected 10 443

18 EIB (n 15).

19 As above.

20 'Rwandan develops app for easy tracing of COVID-19 candidates' <https://furtherafrica.com/2020/05/26/rwandan-develops-app-for-easy-tracing-of-COVID-19-candidates/> (accessed 12 July 2020).

21 As above.

22 As above.

23 www.africanews.com › 2020/07/01 › nigeria-coronavir (accessed 27 August 2020).

victims in the nation, which is nearly 10,2 per cent of the overall deaths in Africa. Notably, South Africa had faced the highest number of casualties on the African continent with 49 413 deaths. As of 23 February 2021 the overall deaths due to COVID-19 in Africa had reached 102 286. On the same date Africa recorded more than 3,87 million cases of COVID-19.²⁴ Even with these mounting numbers of cases, the ongoing argument around a defective COVID-19 tracking system has not stopped, raising many controversial questions as to the accuracy of the reported numbers and the likelihood of under-reporting.²⁵

In Nigeria tracing and isolation of infected people are some of the vital ways of curbing the COVID-19 spread, but still other different methods are currently being explored to ensure an efficient tracking system in the country. However, this is still a very challenging task in a country of over 200 million people with an incapacitated healthcare system and limited experience with the handling of novel diseases.²⁶ Reasonably, technology companies are focusing their creative resources to solve this challenging task by creating applications and platforms that could aid the tracking process and help to report cases across the country.²⁷

In Sierra Leone, for example, an existing unstructured supplementary service data government platform was extended to enable citizens to conduct a self-assessment of their symptoms and get updates on Sierra Leone's COVID-19 situation.²⁸ An additional SMS mobile application that offers users the same functionalities was also developed for smart phone users, and the ability of people to obtain an initial diagnosis not only reassures the population but also helps predict the spread of the virus.²⁹

24 Statista 'Number of coronavirus (COVID-19) deaths in the African continent as of November 18, 2022, by country' <https://www.statista.com/statistics/1170530/coronavirus-deaths-in-africa/> (accessed 24 February 2021)

25 As above.

26 T Obiezu 'Fear & Stigma Keep Nigerians from Helping Contact Tracers' VOA Africa <https://www.voanews.com/africa/fear-stigma-keep-nigerians-helping-contact-tracers> (accessed 27 August 2020).

27 As above.

28 K Ighobor 'Sierra Leonean technologist's app helps to fight COVID-19' <https://www.un.org/africarenewal/magazine/august-2020/sierra-leonean-technologist%E2%80%99s-app-helps-fight-COVID-19> (accessed 12 December 2020)

29 As above.

3 Privacy concerns and debates around COVID-19

Since the dawn of COVID-19, many governments have taken unprecedented measures to track, trace and contain the spread of the pandemic. Tracking the spread of COVID-19 has been done by deploying some digital technologies and advanced analytics to access, collect, process and share data for effective front-line responses. The digital technologies use geo-spatial data, collected through the mobile devices' inbuilt global positioning systems and have helped officials to locate hundreds of thousands of people who might have contracted COVID-19 by interacting with the carriers or attending the virus hotspot locations. These technologies are considered effective for timely, secure and reliable data access and sharing. They form acritical means for understanding the virus and its spread, improving the effectiveness of government policies, and fostering global co-operation in the race to develop and distribute therapies and vaccines.

Some COVID-19 tracking approaches involve digital technologies by using applications that provide a tool for governments to monitor and contain the virus. Through the use of these technologies, governments have been harnessing the power of data to drive digital solutions for effective front-line response concerning the spread of the virus. Tracking the location of newly confirmed cases, rates of recoveries and deaths, and the source of new cases, such as international arrivals or community transmission, have been massively conducted at varying scales. The collection of health data has been crucial in assessing and improving the capacity of national healthcare systems, and in evaluating the effectiveness of containment and mitigation policies that restrict the movement of individuals. It is, thus, proven that digital technologies and advanced analytics are increasingly being developed in order to collect, analyse and share data for front-line responses through the use of geo-location data that is user-derived from mobile call data records or collected from mobile applications; and biometrics for facial recognition data, finger prints, and the like.

The emergence of contact tracing technologies in the fight against COVID-19 in many countries, particularly in Europe and America, has raised privacy and data protection concerns, particularly because privacy and security are important values worthy of attention. The public holds strong privacy concerns about how their personal health data is used. This is especially more so when personal health data is handled and used in a manner that is not directly relevant to providing care. In some cases, not even company employees can fully access the data and link it to a named individual. Privacy concerns arise from the fact that the regulation of fast-moving, rapidly-evolving technologies variably is inadequate and

where it tends to exist, its efficacy remains opaque. It is believed that emerging contact-tracing technologies pose a higher risk to privacy in COVID-19 tracking, thereby violating data privacy policies on preserving the confidentiality, integrity and availability of personal information. Questions on proportionality of the use of contact-tracing applications have been asked touching on fundamental data protection and privacy principles in which information should be accessible only to those authorised to have access.³⁰

There are assumed possible breaches in data utilisation during the COVID-19 crisis. This is because there are fears that contact-tracing applications have been implemented without full transparency, accountability and a commitment to ensuring that data privacy rights of individuals are guaranteed and actually protected. A lack of clear, strong and enforceable data privacy laws across many countries worldwide during COVID-19 tracking creates a fertile environment for massive data privacy breaches by governments, organisations, and individuals involved with tracking, collecting, storing and sharing personal health information. Some COVID-19 tracing approaches have been considered controversial in terms of their potential risk of violating privacy and other fundamental rights of citizens. Particular concerns emerge when such deploying of digital contact-tracing technologies and other physical methods become devoid of transparency, public consultation, and consent of data subjects. Under the framework of information security law, there have been doubts about the integrity of personal health information collected during the contact tracing for COVID-19, particularly in countries that have not adopted enforceable laws on data protection. Data subjects and informed persons have suspected the lack of transparent mechanisms for safeguarding the accuracy and completeness of information and processing methods for protecting personal information against unauthorised modification. Privacy disclosures of personal information are considered as being able to provide governments with ways to monitor and contain the COVID-19 virus. The latter is done by identifying better potential COVID-19 infections and track the spread over time.

It is a given fact that, within a particular health protocol, health information of individuals will be collected, stored and shared by doctors, nurses and other healthcare providers during the treatment of patients. In order to preserve privacy, anonymisation has been used in order to allow

30 See AB Serwin 'Privacy 3.0: The principle of proportionality' (2009) 42 *University of Michigan Journal of Law Reform* 869-890, <https://repository.law.umich.edu/mjlr/vol42/iss4/5> (accessed 12 December 2020); also see HD Gunnarsdóttir and others 'Applying the proportionality principle to COVID-19 antibody testing' (2020) 7 *Journal of Law and the Biosciences* 1-8.

doctors, nurses, hospitals, clinics and other organisations and companies to use and share data without endangering the individual's privacy.³¹ This brings in the concept of using personal data anonymously for intended purposes without linking back to the identity of the data subject. Existing scholarship, however, shows that anonymisation works through de-identification which involves the removal of direct identifiers from the dataset. This technique that blurs and suppresses indirect identifies of a person that may include gender, date of birth, zip code, medical diagnosis, occupation, extreme age, Approximate location ethnicity, uncommon race, and other details by enabling the resultant dataset to be released for consumption as open data is facing fierce criticism. Various technologies are used to ensure that sensitive data is stored on protected remote servers without sharing individual-level data with the data analysts.

Anonymisation requires data analysts to simply send queries to servers for analysing such queries. However, hi-tech engineers have argued that anonymisation that is primarily hinged on privacy is not good during this era of hi-tech as it kills innovation. This debate posits that data privacy regimes should not be used to deter the use of modern technological advances in innovation such as the use of artificial intelligence (AI) that is able to unlock the anonymous information so that hidden data may be used for numerous solutions of scientific problems for social good and economic development.³² For example, nEmesis system in AI helps health departments to identify, for instance, certain restaurants that are the source of illnesses, mainly those that are food-borne.³³ It is further argued that AI is capable of being used to analyse social media data and discover and suggest behavioural and environmental impacts on health. In addition to the nEmesis system described above, examples include tracking of a disease declared a pandemic, such as SARS, influenza or COVID-19 and predicting the likelihood that particular social media users will become ill. The debate here argues that the world should not be entangled or locked in or stuck in the dichotomy of having either innovation or privacy. The contenders of this debate say that such a dichotomy is considered a false one.³⁴

31 YA de Montjoye & A Gadotti 'Moving beyond de-identification will allow us to find a balance between using data and preserving people's privacy' <https://linc.cnil.fr/fr/ya-de-montjoye-and-gadotti-moving-beyond-de-identification-will-allow-us-find-balance-between-using> (accessed 15 September 2020).

32 GD Hager and others 'Artificial intelligence for social good' Computing Community Consortium (CCC), National Science Foundation, 2017 8-9. A Sadilek and others 'Deploying nEmesis: Preventing foodborne illness by data mining social media' Association for the Advancement of Artificial Intelligence 2016.

33 As above.

34 A Sadilek and others 'Deploying nEmesis: Preventing foodborne illness by data

Arguments have it that personal health information is the most sensitive information because it is well associated to an individual's private life. Many countries have numerous suitable and sometimes unsuitable policies, legislation, guidelines, and compliance requirements. All these are key to safeguard health information, privacy and security. However, in Africa, as in many other less-developed parts of the world, data privacy breaches remain key issues for electronic healthcare systems. The privacy of the patient is best protected by implementing a systematic mix of technologies and best practices such as technical de-identification of data and restrictive data access, as well as security measures in the specified technical platforms. Studies have indicated that the use of systematic mix of technologies and best practice have provided security models that make personal data security unauthorised access of protected patient health information extremely improbable, and they may not be compromised.³⁵

Another mixed debate revolves around the legal challenges related to digital contact tracing during COVID-19, including potential risks of harmful acts, lack of privacy, biased algorithms, misinformation, and hacking.³⁶ There is a debate as to the extent to which a right to explanation exists in data privacy. A growing concern is about the practical feasibility of implementing such right in the context of complex data processing such as big data, artificial intelligence and machine learning. In South Africa, big data and deployment of AI has been worked out in several areas, including the healthcare sector, which increases the potential for data mining by social media. It is already underscored that privacy by design as techniques that primarily focus exclusively on protecting confidentiality and the identification of individuals whose data has been accessed, collected, processed, stored and shared is still debated upon as well. Veale, Binns and Ausloos have argued that there is a problem that continues to be debated upon, mainly that the data would still be potentially re-identifiable by third parties with enough capabilities given the automation and artificial intelligence in innovation through technologies.³⁷ Thus, intrusion and the disclosure of personal health information would still be

mining social media' (2017) 38 *AI Magazine* 37-48, <https://doi.org/10.1609/aimag.v38i1.2711> (accessed 20 September 2020).

35 M Puppala and others 'Data security and privacy management in healthcare applications and clinical data warehouse environment' Conference Paper February 2016, doi: 10.1109/BHI.2016.7455821 1-28.

36 <https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/1-a-framework-for-understanding-artificial-intelligence> (accessed 20 September 2020).

37 M Veale, R Binns & J Ausloos 'When data protection by design and data subject rights clash' (2018) 8 *International Data Privacy Law* 105-123, <https://doi.org/10.1093/idpl/ipy002> (accessed 20 September 2020).

a problem because AI allows the processing of personal data in new and unanticipated ways. Other difficulties emanate in the process of identifying specific individuals for linking them with data. This creates challenges of making access, erasure and objection as among the basic rights of the data subject in the process of protecting the data privacy of a person.

Wachter and others³⁸ have doubted the legal basis for the right to an explanation in the *General Data Protection Regulation* (GDPR), particularly in the context of digital data protection where machines process data, consent, collection, and disclosure through automation. They have argued that the right to an explanation is not compatible with the way in which modern machine learning technologies are being developed for production of meaningful information about the logic of processing. They state that it does not help much in the preservation of personal health information. Machine learning systems are designed to discriminate, but some forms of discrimination are socially unacceptable and the systems need to be restrained. The general obligation of fairness in data protection provides the basis for the need to have some level of insight into the functioning of algorithms, particularly in profiling. In this context there are said to be problems in another data privacy issue, namely, transparency in the context of algorithmic accountability. For example, providing the source code of algorithms may not be sufficient and may create other problems in terms of privacy disclosures and the gaming of technical systems. Thus, Wachter and others argue that an auditing approach could be more successful instead by looking at the external inputs and outputs of a decision process, rather than at the inner workings: 'explaining black boxes without opening them'. Their main departure is their proposal to partially decouple transparency as a necessary key step towards accountability and redress. They argue that people attempting to tackle data protection issues have a desire for an action, not for an explanation. The actual value of an explanation will not be to relieve or redress the emotional or economic damage suffered, but to understand why something happened and to help ensure that a mistake does not reoccur.

Another privacy debate, particularly on the African continent, is that privacy protection hinders access of useful information for the public good. This is why data privacy and protection issues in Africa are not a priority for many governments. African governments put much interest in legislation that protects their right to access information from individual

38 S Wachter, B Mittelstadt & L Floridi 'Why a right to explanation of automated decision-making does not exist in the general data protection regulation' (2017) 10 *International Data Privacy Law* 1-25.

persons and organisations, under the guise of national security interests.³⁹ Contenders of privacy rights argue that the right to privacy in many cases has to be balanced against other compelling interests of the state.⁴⁰ Such public interests include the policy agenda of improving the quality of life and promotion of public safety. Thus, public health emergency may override privacy concerns in the interests of the safety of the public.

4 COVID-19 and privacy regulation

As mentioned earlier, tracking COVID-19 raises privacy concerns around the world. During the COVID-19 pandemic, it is witnessed that the interests of public health in many nations overshadows the protection of personal privacy.⁴¹ This has been the practice even in those nations where privacy is protected as a fundamental right in different instruments as well as in constitutions as in European Union (EU).⁴² Moreover, the EU has the stringent privacy protection regime worldwide since 2018 under the General Data Protection Regulation (GDPR) and also through the Directive on Privacy and Electronic Communications (ePrivacy Directive);⁴³ yet it requires its member states to exchange personal data collected through contact tracing. The pandemic exemplifies that the privacy right is not absolute, and it may be limited under some special circumstances, such as the COVID-19 pandemic.⁴⁴ These concerns necessitated the development of new trends of privacy regulation in the context of the COVID-19 pandemic in different regions, sub-regions and nations. These encompass the adoption of new laws, the amendment of the existing laws and the suspension of certain laws.

Globally, the first trend that developed during the COVID-19 pandemic is the adoption of new laws. This was due to the fact that the existing laws were inadequate in responding to the pandemic. This can be seen in some European member countries such as Italy, Switzerland, Australia, Belgium and many others that passed specific laws for protecting privacy

39 A Green 'Scarcity of data protection laws in Africa leaves NGOs exposed' June 2018.

40 BT Sharp 'Right to privacy: Constitutional rights and privacy laws' Live Science Reference Editor 12 June 2013, <https://www.livescience.com/37398-right-to-privacy.html> (accessed 14 September 2020).

41 H van Kolschooten & A de Ruijter 'COVID-19 and privacy in the European Union: A legal perspective on contract tracing' (2020) 41 *Contemporary Security Policy* 479.

42 Art 8 European Convention on Human Rights; Charter of Fundamental Rights of the European Union arts 7 and 8.

43 Consolidated version of the directive on privacy and electronic communications (ePrivacy directive), 2002 OJ (L 201) 37, <https://perma.cc/YHA5-EFXV> (accessed 30 August 2020).

44 ECHR art 8(2) and CFREU art 52.

rights after contract-tracing applications were implemented.⁴⁵ For example, Australia made a temporary human bio-security emergency declaration regarding human corona virus with pandemic potential in March 2020.⁴⁶ It gives the minister responsible expansive powers to set requirements and give directions to combat the pandemic.⁴⁷ The government passed a law on COVID-safe application privacy protections. This is known as Privacy Amendment (Public health Contact Information) Act 2020 and was passed into law on 14 May 2020.⁴⁸ Moreover, Switzerland enacted the temporary Swiss regulation that regulated the organisation, use, operation and data processing by the COVID-19 tracking applications in the country.⁴⁹ In tandem to other countries, Poland also adopted an emergence Bill in March 2020 known as the COVID-19 Act as a response to the pandemic.⁵⁰ In the same vein, the Italian government issued Decree 28, to create a legal framework for processing personal health data by private companies that form part of the health system as well as by the health authorities during the state of emergency.⁵¹ Similarly, the Norwegian government issued a regulation on tracing and epidemic contagion related to COVID-19.⁵²

The second trend that has been adopted in order to protect privacy rights while tracking COVID-19 is an amendment of the existing law. Various states around the globe amended their existing laws so that they can be sufficient in responding to the pandemic. An example of this can be seen from the case of Australia. Despite the fact that Australia adopted some new laws for the pandemic, as explained above, it also amended its Privacy Act in mid-May 2020. The gist of the amendment is to provide stronger privacy protections for the users of the COVIDSafe application and data collected through the application, and also to criminalise the use of data

45 L Edwards 'Apps, politics and power: Protecting rights with legal and software code' in L Taylor and others (eds) *Data justice and COVID-19: Global perspectives* (2020) 43.

46 Privacy Amendment (Public Health Contact Information) Act 2020, <http://www.legislation.gov.au/Details/C20202A00044> (accessed 30 August 2020).

47 H Maclean & K Elphick 'COVID-19 legislative response – Human biosecurity emergency declaration explainer' *Flagpost parliamentary library*, <http://perma.cc/Y473-TWXT> (accessed 18 September 2020).

48 Parliament of Australia Privacy Amendment (Public Health Contact Information) Bill 2020, <https://perma.cc/UK7M-DY6Y> (accessed 16 September 2020).

49 Switzerland 'Regulation on proximity tracing app pilot adopted' <http://www.loc.gov/law/foreign-new/article/switzerland-regulation-on-proximity-tracing-app-pilot-adopted> (accessed 18 September 2020).

50 <http://prawo.sejm.gov.pl/sap.nsf/download.asp/WDU20200000374/O/D20200374.pdf> (accessed 17 September 2020).

51 OECD 'Ensuring data privacy as we battle COVID-19' (2020), <http://www.oecd.org/policy-responses> (accessed 17 September 2020).

52 *Forskrift om digital smittesporing og epidemikontroll I anledning utbrudd av COVID-91* (FOR 2020 03 27-475), <https://perma.cc/UKS8-5Y5W> (accessed 14 September 2020).

collected by the tracking-up for uses other rather than contact tracing.⁵³ Another example of a country that amended its laws so as to facilitate tracking COVID-19 is Poland. It amended the Telecommunication Act⁵⁴ and, hence, allowed the Minister of digital to have access to the location data of quarantined and infected persons from the telecommunication service providers.⁵⁵

In the same vein, in order to fight COVID-19 some other countries suspended some existing legislation that was regarded as an impediment to fighting the pandemic. Some of these laws provide for the right to privacy. Hungary is an example of the countries that suspended privacy right of individuals in fighting COVID-19. In so doing, the government in March 2020 issued a decree allowing the Minister for Innovation and Technology to access all data available, personal data inclusive, without limits.⁵⁶ Further, in April 2020 it also issued another decree allowing staffs of a body set up for the defence against coronavirus to be granted access to information from any entity upon request in order to implement their duties.⁵⁷ Among other things, such information included health, contact personal identification and register data.⁵⁸ Conversely, there was no provision in the decree providing for the limitation of the access for the protection of privacy of the individuals. In tandem with this, the same government issued a decree in May 2020 suspending the application of the General Data Protection Regulation and the domestic Privacy Act (especially provisions dealing with the rights of data subjects, such as the right to information, erasure, objection, and so forth) until the end of the state of perceived or experienced danger, which may not necessarily be coronavirus pandemic.

Privacy challenges arising from tracking COVID-19 in other parts of the world are also experienced in Africa. Besides, its impact is more prominent in Africa due to the fact that only 30 out of 55 countries in

53 Privacy Amendment (Public Health Contact Information) Bill 2020 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd098 (accessed 14 September 2020)

54 <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800> as amended (accessed 18 September 2020).

55 M Brewczynska 'Policing quarantine via app' in Taylor and others (n 4) 234.

56 <https://magyarkozlony.hu/dokumentumok/c4210b08dd73832b3ca261193f85d58498c9718/megtekintes> (accessed 17 September 2020).

57 <https://magyarkozlony.hu/dokumentumok/13285bbde75a626ff044ec795e70a6ee5d700b29/megtekintes> (accessed 17 September 2020).

58 I Borocz 'Suspending rights and freedoms in a pandemic induced state of danger' in Taylor and others (n 45) 146.

Africa variably adopted data privacy laws.⁵⁹ Most of these laws follow the spirit of the repealed EU Data Protection Directive, 1995. This implies that they are not in line with the current technological development. Similarly, most of the existing laws have not entered into force and some data protection authorities are yet to be appointed.

Due to the privacy challenges brought about by contact tracking during COVID-19, some countries in Africa resorted to the adoption of new laws so as to protect privacy. Others resorted to the amendment the existing laws while others suspended some laws that were regarded as an impediment in tracking COVID-19. However, other countries decided to use digital tracking of COVID-19 without having any law for the protection of the privacy of individuals.

To date, particularly in Africa, the important parts of the private lives of victims of COVID-19 have been suspected to have been intruded contrary to the fundamental right to privacy.⁶⁰ A substantial amount of data was randomly and widely collected in an unlimited pattern through a combination of a variety of COVID-19 tracking approaches. These included physical contact tracing, oral questioning through face-to-face interviews, the application of digital technologies such as the use of mobile phones, applications, geolocation data, and so forth. It is in this context that we contend that tracking COVID-19 has both negative and positive implications for data privacy in Africa.

Largely, health information has been and continues to be collected, processed, stored and shared without clear and enforceable data privacy laws in Africa. Only a few countries in Africa have functioning data protection legislation. For example, South Africa has the Protection of Personal Information Act (POPIA).⁶¹ Thus, POPIA is South Africa's law on data protection that seeks to give effect to the constitutional right to privacy by putting in place conditions that have to be complied with by authorised parties involved in the extraction and processing of personal information.

59 CIPESA 'Mapping and analysis of Privacy Laws and Policies in Africa-Summary Report' (July 2021) 5 <https://cipesa.org/wp-content/files/reports/Mapping-and-Analysis-of-Privacy-Laws-and-Policies-in-Africa.pdf> (accessed 11 October 2020).

60 M Muson 'Contact tracing and data protection during COVID-19 pandemic in South Africa', <https://blogdroiteuropeen.com/2020/07/29/contact-tracing-and-data-protection-during-COVID-19-pandemic-in-south-africa-by-melody-muson/> (accessed 15 September 2020).

61 Act 4 of 2013.

In Mauritius, the Data Protection Act 2017 (DPA) governs some exceptional measures that involve the processing of various types of personal health data of the individual, including body temperature, other health data, geolocation data, and so forth. During the COVID-19 pandemic, Mauritius permitted hypermarkets, supermarkets, superettes and food retail shops or food outlets to take the body temperature of their customers. Regulations were passed on who can take the temperature and to whom the temperature can be communicated. Also, Mauritius has the Prevention and Mitigation of the Infectious Disease (Coronavirus) Regulations 2020, which itself is made under section 79 of the Public Health Act. Under the said regulations, the General Notice (GN) 547 of 2020 enacted under Regulation 13(2) of the Regulations contains conditions for reopening and operation of food outlets in Mauritius. The body temperature of each customer may be taken by staff of the relevant food outlet. Where any customer has a high temperature (38 degrees and above), the law provides that the customer will be transferred to the nearest hospital and he will be dealt with according to the protocol of the Ministry of Health and Wellness. The General Notice directs the taking of temperature to be done as from Thursday 2 April 2020 until 15 April 2020 and, upon expiry of that period, a new regulation would need to be enacted to extend this duration so that this practice may lawfully continue beyond the earlier date issued, that is to say 15 April 2020.

Mauritius went further by providing the duty to explain to the customer the reason and purpose for collecting the data. The person collecting information must state to which authority the information will be communicated. A categorical statement of the right of the data subject has to be stated and the period of retention of such data. An individual has the right to lodge a complaint with the Data Protection Commissioner in situations where they are not satisfied with the way in which their personal data is being processed. The easy accessibility of collected information should be stated in clear and plain language, and so forth.

Despite efforts made by a few African countries, it is highly doubtful whether there can be a reliable guarantee of the protection of personal health data in most African countries. In most African countries, data is shared without legislation to govern data privacy, information processing and sharing. Personal data is collected and used without securing specific and unambiguous consent of data subjects. There is massive unauthorised sharing of health information by organisations that collect and use such information.

Generally, in Africa, a few countries, such as South Africa and Mauritius, have frameworks in place to support extraordinary COVID-19

control measures in ways that are relatively fast, scalable and, to some extent, in compliance with existing privacy and data protection regulations within certain provided framework of protection of rights of data subjects. However, security and trustworthiness of legal mechanisms remain to be seen as citizens from these countries and literature have shown that there are still some dangers of a clash between data protection and data subjects' rights.⁶²

Ghana is an example of a country with privacy protection regulation, but which went further and adopted a new legislation to combat the COVID-19 pandemic.⁶³ It passed an Executive Instrument (EI) 63 – the Establishment of Emergence Communication System Instrument in March 2020 – which provides, among other things, for the establishment of an emergency communication system to trace all contacts of persons suspected of or affected by a public health emergence, COVID-19 inclusive. However, the instrument is very wide as it does not define the public emergencies in which the law can be applicable. Also, the instrument does not restrict its applicability to the COVID-19 pandemic and, hence, instead of protecting privacy during the COVID-19 crisis, it legalises impending intrusive state surveillance in the long run. It is also interesting to note that while public emergencies fall under the state of exception, the instrument seems to be laying down a permanent registry without providing any safeguards. Consequently, it may amount to a permanent threat to individuals' data privacy rights.⁶⁴ It is worth noting that the EI instrument in Ghana was used to suspend the applicability of the existing laws that makes the monitoring of personal communications by state and security actors subject to a court warrant.

Another example is that of South Africa, a country with an incomplete data protection landscape. The Protection of Personal Information Act was adopted in 2013, but it has not yet fully entered into force. However, most of its provisions only came into force in July 2020 with a grace period of one year for data processors to comply.⁶⁵ In the response to the COVID-19 pandemic, the minister responsible issued a regulation geared to expand the state's powers for mining personal data from the citizen. This raises concerns over whether this mining adheres to privacy protection principles.

62 M Veale, R Binns & J Ausloos 'When data protection by design and data subject rights clash' *International Data Privacy Law*, <http://doi.org/10.1093/idpl/ipy002> (accessed 15 September 2020).

63 Ghana, <http://www.news.itu.int/ghana-launches-COVID-19-tracker-app> (accessed 17 September 2020).

64 S Oduro-Marfo 'Transient crisis, permanent registries' in Taylor and others (n 45) 141.

65 A Gillwald and others 'Protecting mobile user data in contact tracing' in Taylor and others (n 45) 250.

The government went further and amended the regulations of its Disaster Management Act to allow telecommunication service providers to provide geolocation data to health authorities for contact-tracing purposes only.⁶⁶ The new regulation is known as the disaster management contact-tracing regulation. Among other things, the regulation limits the scope of mobile data collection by a COVID-19-tracing data base to only those individuals that are suspected of or known to have come into contact with anyone who is suspected of or already is infected with the corona virus. The regulation encompasses some privacy protection principles in data collection. These include collecting data for specific purposes, accuracy of data, accountability of the collecting parties and limitation on the retention of data. However, the regulation is in conflict with other laws in the country that require a judge's order for communication interception as the regulation does not require such an order.⁶⁷

Another example is Nigeria, a country with a complete data protection framework with a Data Protection Regulation since 2019 (NDPR).⁶⁸ In tracking COVID-19, Nigeria invoked the provisions of the NDPR to legitimise the collection and sharing of personal information.⁶⁹ The Act provides that a person's data may only be collected and disclosed under any of the following conditions: 'when the processing is required for the protection of the vital interest of a data subject or another natural person; or if the processing is necessary for the performance of a task carried out in the public interest'.⁷⁰

Relying on the provision above, the Nigerian government authorised the use of the contact-tracking application for COVID-19 without enacting any new law or amending the existing. However, this practice proves to be detrimental to privacy right protection to Nigerians, taking into consideration how the applications are working. The same was the practice in countries such as Kenya. Moreover, there is another category of countries that used the COVID-19 tracking application without having a data protection regulation in force, for example, Botswana.⁷¹

66 As above.

67 Gillward and others (n 65) 251.

68 Nigerian Data Protection Regulation, 2019.

69 D Oturu 'Nigeria COVID-19 coping with data protection/privacy challenges within the context of the Nigerian data protection regulation' <https://www.mondaq.com/nigeria/data-protection/910792/covid-19-coping-with-data-protectionprivacy-challenges-within-the-context-of-the-nigerian-data-protection-regulation> (accessed 18 September 2020).

70 Nigerian Data Protection Regulations sec 2.2.

71 Botswana 'Data protection overview' <https://www.dataguidance.com/notes/botswana-data-protection-overview> (accessed 18 September 2020).

5 Conclusion

The discussion above demonstrates the difficulty with which jurisdictions around the world have struggled to fight COVID-19 while variably trying to ensure the protection of the fundamental rights of individuals. Nonetheless, a variation of legal approaches to the regulation of privacy in Africa and beyond has left it open for possibilities by governments, private sectors and individuals to infringe the right to privacy of individuals. In Africa, where data protection regulation in general is still emerging, and with limited data privacy practices, it has become more challenging to guarantee individuals' right to privacy. A common approach by African states could have helped to mitigate the difficulty of cross-border enforcement of data privacy.

References

- Edwards, L 'Apps, Politics and Power: Protecting Rights with Legal and Software Code in Taylor, L and others (eds) *Data justice and COVID-19: Global perspectives* (2020) 40
- Gregory, DH and others 'Artificial Intelligence for Social Good Computing Community Consortium (CCC), National Science Foundation (2017)
- Gunnarsdóttir, HD and others 'Applying the proportionality principle to COVID-19 antibody testing' (2020) 7 *Journal of Law and the Biosciences* 1
- Hripcsak, G and Albers, DJ 'Correlating electronic health record concepts with healthcare process events'(2013) *Journal of the American Medical Informatics Association* 20(e2), pp.e311-e318, 2013 (accessed 27 September 2021)
- Lu, H and others 'Outbreak of pneum\onia of unknown etiology in Wuhan, China: The mystery and the miracle' (2020) 92 *Journal of Medical Virology* 401
- Macleane, H & Elphick, K 'COVID-19 legislative response – human biosecurity emergency declaration explainer' Flagpost parliamentary library<http://perma.cc/Y473-TWXT>
- Oduro-Marfo, S 'Transient crisis, permanent registries' in Taylor, L and others (eds) *Data justice and COVID-19: Global perspectives* (Meatspace Press, 2020)
- Paxton , Cand others 'Developing predictive models using electronic medical records: challenges and pitfalls. In AMIA Annual Symposium proceedings (pp 1109-1115), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900132> (accessed 21 October 2020)
- Sadilek, A and others 'Deploying nEmesis: Preventing Foodborne Illness by Data Mining Social Media' (2016) 38 *AI Magazine* 37
- Serwin, BA 'Privacy 3.0: The Principle of Proportionality' (2009) 42 *University of Michigan Journal of Law Reform* 869
- van Kolschooten, H & de Ruijter, A 'COVID-19 and privacy in the European Union: A legal perspective on contract tracing' (2020) 41 *Contemporary Security Policy* 479
- Veale, M and others 'When data protection by design and data subject rights clash' (2018) 8 *International Data Privacy Law* 105
- Wachter, S and others 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2016) 7 *International Data Privacy Law* 1

YA de Montjoye and Gadotti, A 'Moving beyond de-identification will allow us to find a balance between using data and preserving people's privacy' <https://linc.cnil.fr/fr/ya-de-montjoye-and-gadotti-moving-beyond-de-identification-will-allow-us-find-balance-between-using> (accessed 27 September 2021)

10

CAN WE TRUST BIG BROTHER? A CRITIQUE OF DATA PROTECTION MEASURES IN SOUTH AFRICA'S COVID-19 TRACING DATABASE

Dusty-Lee Donnelly

Abstract

This chapter scrutinizes the South African government's response to the COVID-19 pandemic, focusing on data collection and the establishment of a COVID-19 tracing database under the Disaster Management Act. Critically analysing the regulations, it underscores sweeping provisions and inadequate guidance from the Information Regulator, especially regarding location tracking. The chapter provides an in-depth examination of POPIA's key principles – accountability, reasonableness, minimality, purpose specification, storage limitation, openness, and data subject participation – highlighting their application in the context of pandemic-driven data governance.

A trenchant critique explores the illusion of anonymization as a safeguard and cautions against unwarranted mass surveillance, raising concerns about citizens' privacy protection. The chapter concludes by contemplating the future of COVID-19 research, examining legal pathways for conducting scientific research under POPIA. It analyses the exemption from informed consent requirements in sections 15 and 27(1)(d), comparing it to the more stringent provisions of the public interest exemption in section 37, and questions whether adequate measures were taken to safeguard citizen privacy amidst the pandemic's data-driven response.

1 Introduction

On Thursday 5 March 2020 the first positive result for severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) was identified by the National Institute for Communicable Diseases in a small town in KwaZulu-Natal. COVID-19 had arrived in South Africa.

To keep the public informed of developments, the then Minister of Health, Dr Zweli Mkhize, issued a press briefing on the same date.¹ He did

1 National Institute for Communicable Diseases 'First case of COVID-19 coronavirus reported in SA' 5 March 2020, <https://www.nicd.ac.za/first-case-of-covid-19-coronavirus-reported-in-sa/> (accessed 11 October 2021).

not name the patient, but provided enough personal information about the patient² that within a day the patient, his family, their doctor, the name of the town where they lived, and the school attended by their children were public knowledge.³ While there were regrettable reported incidents of hate mail directed at the couple, the provision of clear information was critical when very little was known of the virus, and the potential for the public to panic was extremely high.

This incident brought into sharp focus the dichotomy between the right to privacy and the public's interest in a free flow of information about the virus and its spread. Section 2 of the Protection of Personal Information Act 4 of 2013 (POPIA) makes it clear that the Act is not focused solely on the protection of individual privacy but aims to strike a balance between the protection of privacy, through safeguarding personal information, and the protection of other rights, such as the right of access to information, and vital interests such as the free flow of information within and across our borders.⁴

While data protection laws are nothing new, the scale and speed of transition to widespread reliance on digital data processing during the COVID-19 pandemic makes a fresh analysis of data protection measures all the more urgent. The glut of digital data available today, and new computational techniques for the analysis of 'big data' using complex algorithms and artificial intelligence, have set new precedents in the public health and research sector. Likewise, restrictions on movement have meant that digital platforms have played an exponentially important role in all areas of work, education, and social life.

This chapter will discuss the South African government's use of data, including mobile-location data, to track citizens and monitor the spread of COVID-19. The government passed regulations under the

2 As defined in sec 1 of the Protection of Personal Information Act 4 of 2013 (POPIA). The personal information supplied included the patient's age, general, marital status, number of children, most recent travel location and number in the travel party, and the patient's medical history (symptoms, date and nature of treatment).

3 K Singh 'Coronavirus: Authorities pull out all stops, high-level meeting planned with KZN school' 6 March 2020, <https://www.news24.com/news24/SouthAfrica/News/coronavirus-authorities-pull-out-all-stops-high-level-meeting-planned-with-kzn-school-20200306> (accessed 11 October 2021).

4 POPIA sec 2(a) reads: 'The purpose of this Act is to (a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at (i) balancing the right to privacy against other rights, particularly the right of access to information; and (ii) protecting important interests, including the free flow of information within the Republic and across international borders.'

Disaster Management Act⁵ that provided for the creation of a COVID-19 'contact-tracing' database. Although 'contract tracing' is not defined in the regulations, it refers to the process of tracking and monitoring individuals who may have come into contact with a person infected with COVID-19. The objective of contact tracing is to notify individuals of their exposure (that is, close contact) to a known or suspected COVID-19-positive patient, thus breaking the chain of transmission as soon as possible.⁶

There is scientific support for the use of mobile location data to track and forecast the spread of COVID-19,⁷ building on earlier studies that had begun to use mobile location data in response to Haiti's cholera outbreak in 2010⁸ and the spread of the Ebola virus and Zika virus.⁹ However, the absolute imperative of accurate real-time monitoring to track the spread of the virus and monitor the efficacy of interventions cannot overshadow the need for caution. In any instance where a government employs mass surveillance of its citizens, it must ensure that it does not do so 'for purposes unrelated to the pandemic'¹⁰ and acts with due regard for the right to privacy.

2 Government response to COVID-19

COVID-19 soon spread rapidly in South Africa. In response to the pandemic, the government declared a state of national disaster on 15

5 Act 57 of 2002.

6 European Data Protection Board 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' 21 April 2020 3, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en (accessed 11 October 2021).

7 I Marcello & E Vayena 'On the responsible use of digital data to tackle the COVID-19 pandemic' (2020) 26 *Nature Medicine* 463, describing a study that forecast COVID-19 spread using location-services data collected by the WeChat app, in combination with the Official Aviation Guide, a worldwide database of airline booking schedules. See JT Wu and others 'Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: A modelling study' (2020) 395.1022 *The Lancet* 689.

8 L Bengtsson and others 'Using mobile phone data to predict the spatial spread of cholera' (2015) 5 *Scientific Reports* 1. The study collected anonymised data of the location of the last outgoing call or text message each day for 2,9 million users of Haiti's largest mobile operator over a period of two months.

9 M Bates 'Tracking disease: Digital epidemiology offers new promise in predicting outbreaks' (2017) 8 *IEEE pulse* 18. Web-based 'bio-surveillance' uses a variety of techniques to mine information on the web, such as news reports, Twitter and other social media posts, and web searches, to track or forecast disease spread.

10 United Nations 'COVID-19: We are all in the this together' April 2020 3, https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un_-_human_rights_and_covid_april_2020.pdf (accessed 11 October 2021).

March 2020.¹¹ On 18 March 2020 the government issued the first tranche of regulations under section 27(2) of the Disaster Management Act 57 of 2002 (Regulations).¹² On 23 March 2020 the President of the Republic of South Africa announced that the National Coronavirus Command Council had decided to enforce a nation-wide lockdown.¹³ At the time of writing, South Africa has been in lockdown, at varying levels of restrictiveness, for 19 months. The latest extension of the national state of disaster runs until 15 November 2021, with no indication of when or how it will finally be brought to an end.¹⁴

2.1 Collection of COVID-19 data

Almost immediately, the government set up a high-level advisory panel of scientific experts to develop evidence-based responses to the pandemic,¹⁵ and from the outset there was a strong focus on collecting data from several sources. Twenty-eight thousand community health workers were re-deployed to do door-to-door visits to identify COVID-19 symptomatic cases, refer for testing and monitor compliance with quarantine restrictions.¹⁶ During these screening visits, a mobile phone application, Covid Connect, was used to upload household data, symptoms and location coordinates to a central database and thus enable accurate mapping of screening coverage.¹⁷ While community screening was rapidly criticised as unsustainable and unreliable given the high levels of asymptomatic patients,¹⁸ it was reported that over 11 million people (around 20 per cent

11 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Declaration of National State of Disaster' Gov Notice 313 in *Government Gazette* 43096 of 15 March 2020.

12 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Regulations issued in terms of section 27(2) of the Disaster Management Act, 2002' Gov Notice 318 in *Government Gazette* 43107 of 18 March 2020.

13 President of the Republic of South Africa, C Ramaphosa 'Statement by President Cyril Ramaphosa on Escalation of Measures to Combat COVID-19 Epidemic' 23 March 2020, <http://www.dirco.gov.za/docs/speeches/2020/cram0323.pdf> (accessed 11 October 2021).

14 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Extension of a National State of Disaster (COVID-19)' Gov Notice R1031 in *Government Gazette* 45313 of 13 October 2021.

15 SS Abdool Karim 'The South African response to the pandemic' (2020) 382 *New England Journal of Medicine* e95.

16 As above.

17 As above.

18 M Mendelson & S Madhi 'South Africa's coronavirus testing strategy is broken and not fit for purpose: It's time for a change' (2020) 110 *South African Medical Journal* 429.

of the population) had been screened,¹⁹ raising questions about the privacy and security of the data collected.

Free mobile tools for voluntary self-screening emerged,²⁰ and mandatory screening was implemented for all employees entering places of work²¹ and learners, teachers and visitors at schools.²² In addition, mobile applications for receiving exposure notifications were soon launched for both iOS and Android devices,²³ with mixed reviews regarding their privacy assurances²⁴ and efficacy as contact tracing tools.²⁵

In addition, the results of all positive COVID-19 diagnostic tests²⁶ and rapid screening²⁷ in both the private and public sectors were communicated to the National Health Laboratory Service (NHLS).²⁸ These results were used to identify localised outbreaks and map hot spots for targeted lockdown regulations.²⁹ While the accuracy of the geo-spatial mapping of viral spread in real-time was severely hampered by delays in laboratory

19 Abdool Karim (n 15).

20 Business for SA 'South Africans encouraged to use COVID-19 digital health assessment tool' 8 June 2020, <https://www.businessforSA.org/south-africans-encouraged-to-use-covid-19-digital-health-assessment-tool/> (accessed 11 October 2021). The National Department of Health made the symptom checker available using USSD via its dedicated COVID-19 Whatsapp chat service.

21 Minister of Employment and Labour, Thembelani Waltermade Nxesi 'COVID-19 occupational health and safety measures in workplaces' Gov Notice 479 in *Government Gazette* 43257 of 29 April 2021.

22 Department of Basic Education 'Standard Operating Procedures', https://www.nicd.ac.za/wp-content/uploads/2020/11/Revised-DBE-guidelines-Management-of-COVID-in-schools_Sept2020.pdf (accessed 11 October 2021).

23 D Johnson 'Assessment of contact tracing options for South Africa' (October 2020) Research ICT Africa Cape Town, <https://researchictafrica.net/wp/wp-content/uploads/2020/10/Contact-tracing-survey-report-David-Johnson-Oct2020.pdf> (accessed 11 October 2021).

24 L Bradford and others 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 34.

25 IM Viljoen and others 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 *South African Journal of Bioethics Law* 21 argue that it is not viable in South Africa where 'many people do not have smartphones'. For a full discussion of the barriers to uptake, including smartphone penetration, data costs and required download rates for effective contact tracking, see Johnson (n 23) 1-2.

26 The reverse transcriptasepolymerase chain reaction (RT-PCR) test.

27 SARS-COV-2 rapid antigen and antibody tests.

28 National Health Laboratory Service 'COVID-19 surveillance reports', <https://www.nicd.ac.za/diseases-a-z-index/disease-index-covid-19/surveillance-reports/> (accessed 18 October 2021).

29 Abdool Karim (n 15).

test turnaround time and a lack of uniformity in rates of testing,³⁰ the National Department of Health has continued to provide the public with daily statistics of new infections and deaths and regular regional updates on testing, rates of infection, recoveries, deaths, and more recently, vaccinations.³¹

2.2 COVID-19 tracing database

Additional data collection measures were implemented from 2 April 2020, when a COVID-19 tracing database was created by amendment of the regulations.³² The new regulation 11H made it mandatory for every person being tested for COVID-19 to disclose a set of personal information comprising the person's first name, surname, identity or passport number, residential address, other addresses at which the person could be located, cellular telephone number and a copy of photographic identification (such as identity book, identity card or passport). In addition, they were required to disclose the names and contact details of all persons with whom they had known or suspected close contact.³³ Every testing site was obliged to collect these particulars insofar as they were available when administering the test.³⁴ In every case of a positive COVID-19 result, the person's personal information, their result, and the personal information of their contacts are communicated by the laboratory and the NICD to the Director-General: Health for inclusion in the COVID-19 contact-tracing database.

The regulations also contained measures to monitor the movement of persons. The same set of personal information was to be collected for all persons staying at accommodation establishments set up for essential services workers, quarantine, isolation and those stranded under the hard lockdown (when travel restrictions prevented persons returning home in certain cases) and included in the database.³⁵ Furthermore, the Director-General: Health was authorised to requisition mobile-location data from electronic communication service providers regarding 'the locations or movements of any person known or reasonably suspected to have

30 Mendelson & Madhi (n18) 429.

31 National Department of Health 'COVID-19 online resources and news portal', <https://sacoronavirus.co.za/> (accessed 11 October 2021).

32 Minister of Cooperative Governance and Traditional Affairs, Dr NC Dlamini-Zuma 'Disaster Management Act, 2002, Amended of regulations issued in terms of section 27(2)' Gov Notice R446 in *Government Gazette* 43199 of 2 April 2020.

33 Regulation 11H (3)(a)-(c).

34 Regulation 11H (6).

35 Regulation 11H (9) read with Annexure D to the regulations.

contracted COVID-19, and 'any person known or reasonably suspected to have come into contact [with them]'.³⁶ These were sweeping provisions that were rightly cause for close scrutiny.

2.3 Guidance from the Information Regulator

In response to the need for clarity on data protection issues, the Information Regulator of South Africa issued a guidance note on data protection during the pandemic on 3 April 2020.³⁷ At the time POPIA had not yet come into full force.³⁸ Nevertheless, the Information Regulator 'encourage[d] proactive compliance by responsible parties when processing personal information of data subjects who have tested or are infected with COVID-19, or who have been in contact with such data subjects'.³⁹

At the same time the Information Regulator recognised that effective management of the spread of COVID-19 'has necessitated the limitation of various constitutional rights of data subjects', and 'supports the need to process personal information of data subjects in order to curb the spread of COVID-19'.⁴⁰

While the Information Regulator's response was timely, it was disappointingly thin on detail. Although the guidance note recorded that the regulations should be implemented 'in conjunction with' the conditions for lawful processing of personal information⁴¹ there was no actual guidance on the extent to which the regulations in fact complied with the conditions for lawful processing, or on whether limitations to the right to privacy were in fact constitutionally justifiable in scope.

36 Regulation 11H (10).

37 Information Regulator of South Africa 'Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 Of 2013 (POPIA)' 3 April 2020, <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf> (accessed 11 October 2021).

38 The commencement of the operative provisions of POPIA took place on 1 July 2020 in terms of Proclamation R21 of 2020 in *Government Gazette* 43461 of 22 June 2020. In terms of sec 114(1) of POPIA a one-year grace period to bring all processing into line with the Act applied until 30 June 2021.

39 Information Regulator (n 37) para 2.1.

40 Information Regulator (n 37) para 2.3.

41 Information Regulator (n 37) para 9.

3 Protection of personal information

3.1 Processing health data as special personal information

Information pertaining to a data subject's health is included in the definition of special personal information.⁴² Processing of such information is prohibited without a lawful ground of authorisation.⁴³ The first general authorisation for processing special personal information requires that the data subject (or their parent or guardian in the case of a child) has given consent for the processing.⁴⁴ However, a number of other general and specific authorisations for processing are set out.

In the context of the COVID-19 pandemic, the most relevant would be that the party was processing the personal information, including health information, in order to comply with a legal obligation imposed by the regulations.⁴⁵ The general authorisation for research conducted in the public interest is discussed later in this chapter. In addition, the processing of health data is specifically authorised by POPIA in a number of specific use cases, including patient treatment and care, and the administration of health care institutions,⁴⁶ and by insurance companies and medical schemes,⁴⁷ schools⁴⁸ and employers.⁴⁹

3.2 Defining location information as personal information

POPIA includes 'location information' in the definition of personal information in section 1 of the Act. Such data must therefore be processed

42 POPIA sec 1.

43 POPIA sec 26.

44 POPIA sec 27(1)(a).

45 POPIA sec 27(1)(b) authorises the processing of any special personal information where the 'processing is necessary for the establishment, exercise or defence of a right or obligation in law'. Similarly, see the general justification for processing any other personal information under sec 11(1)(c).

46 POPIA sec 32(1)(a).

47 POPIA sec 32(1)(b), although a data subject's right to object to processing is specifically preserved in relation to the use of health data for purposes of 'risk assessment'.

48 POPIA sec 31(1)(c), insofar as is necessary to accommodate a pupil's special needs or make special arrangements concerning their health.

49 POPIA sec 31(1)(d). The provisions can be interpreted to include collection of health data where relevant to the administration of pension schemes and funeral benefits, as well as the support and reintegration arrangements made for workers self-isolating or with co-morbidities that might require special arrangements to work from home during the COVID-19 pandemic.

in full compliance with the conditions for lawful processing set out in the Act. The term 'location information' is not further defined in POPIA, but when read with the general definition of personal information, it should be interpreted to mean any data that reveals the geographic position of the data subject, with a sufficient degree of proximity that their identity can be revealed or it might reveal other personal information about them. For example, location information might reveal where a person lives or works, and a visit to a medical testing facility might reveal the data subject's medical history or likely medical condition.

In the COVID-19 context government tracked location information manually and electronically. Manual entries in paper-based or electronic patient health records at the time of any testing for COVID-19 included the patient's home address and recent close contacts, and were required by law to be transmitted with the patient's name, identity number, contact details and test results to the NICD. Both the NICD and the entity administering the test would be a responsible party and as such fully accountable for full compliance with POPIA in respect of its processing of that personal information.

However, the real concern was with location tracking of citizens in (near) real time using the location data collected by electronic communication service providers, such as mobile cellular network providers. The regulations⁵⁰ provided:

The Director-General: Health may, in writing and without prior notice to the person concerned, direct an electronic communications service provider licensed under the Electronic Communications Act, 2005 (Act No 36 of 2005) to provide him or her, for inclusion in the COVID-19 Tracing Database, with such information as that electronic communications service provider has available to it regarding –

- (a) the location or movements of any person known or reasonably suspected to have contracted COVID-19; and
- (b) the location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated, with a person contemplated in subparagraph (a),
and the electronic communications service provider must promptly comply with the directive concerned.

50 Regulation 11H (10).

In this context, the term ‘location data’ refers to information that reveals the geographic position of the user’s device. This is still personal information as it may be inferred that the location(s) or movement(s) of the device provide information about the location(s) or movement(s) of the device user.⁵¹ There are two principal ways in which mobile location data can be collected: mobile location tracking and network-based location tracking. In both cases, collection can be carried out at least partly undetected and is not well understood by device users, heightening mistrust.

3.2.1 *Mobile location tracking*

Firstly, mobile applications installed on smart devices, such as smartphones and tablets, can track location using the on-device GPS sensor. An application user has some control over location tracking as they must grant an application permission to access location and can also turn off location services in the device system settings. What may be less clear to the application user is whether the application is monitoring location only when the application is in use, or continuously by way of a background process. Further application users may not understand the practical difference between the course-grained and fine-grained instantiation of location data collection by the application. Further, even if location services are turned off, it is possible to passively track location and the proximity of devices to one another, using wireless network (WLAN)⁵² and Bluetooth⁵³ connections by collecting the identification code of the wireless access point or Bluetooth beacon and signal strength (as a proxy for proximity of the device and the duration of proximity).

These are the types of location information used by contract tracing mobile applications such as Covid Connect, COVI-ID and COVID-ALERT.⁵⁴ The privacy of users of such applications may differ greatly. For example, it is reported that in China the contact-tracing application ‘Health Code’ generates a code that is required to access homes, shopping centres, businesses and public transport. As using the application is mandatory, it

51 See eg the definition in the European Union’s Privacy and Electronic Communications Directive 2002/58/EC. Art 2(c) and rec 14: ‘any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’.

52 See eg *United States v InMobi Pte Ltd* Case 3:16-cv-03474 (ND Cal June 22, 2016).

53 Bengtsson (n 8) 1.

54 Johnson (n 23) 20-23.

has 700 million users. GPS and Bluetooth location data are collected and the application reportedly shares this information with the police.⁵⁵

In contrast, the COVID-ALERT application developed by the South African National Department of Health uses the exposure notification framework developed by Google and Apple. The application is designed to protect privacy by sending a randomised Bluetooth identification beacon (that changes every 10 minutes) to other devices in close proximity that also have the application installed. Data is stored on the user's device, not a central server, and is only stored for 14 days. A user, upon receiving a positive COVID-19 diagnosis, can then choose to upload the anonymous Bluetooth codes to the central server that would deliver them to every device that had registered them in the last 14 days. At no point is any person identified.⁵⁶

3.2.2 *Network-based location tracking*

Second, network-based location tracking refers to a form of location tracking enabled by cell site location information collected by cellular network operators (electronic communications service providers) through the continuous connection of the mobile phone to radio antennae positioned on cell towers, from which the mobile phone obtains its signal and on which its functionality depends.⁵⁷ While less accurate than GPS, being approximate to the radius of the tower's signal coverage,⁵⁸ by triangulating the signal, greater accuracy is obtained, and the connection automatically generates a time-stamped record of these connections.⁵⁹

The term 'historical' or 'archived' cell site location information thus refers to this record of past movements, that is automatically being collected and stored about every cell phone user. The term 'real-time' data relates to tracking in the present moment on an ongoing basis.

55 M Wang 'China: Fighting COVID-19 with automated tyranny' *The Diplomat* 1 April 2020, <https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny/> (accessed 18 October 2021).

56 National Department of Health 'COVID Alert SA app: Data protection and privacy policy', <https://sacoronavirus.co.za/covidalert/privacy-policy/> (accessed 18 October 2021).

57 It is the form of tracking that led to the landmark US decision in *Carpenter v United States* 585 US (2018) which held that obtaining historical cell site location information without a warrant violated 4th amendment rights.

58 On average one to ten kilometres squared.

59 D Donnelly 'Privacy by (re)design: A comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law' PhD thesis, University of KwaZulu-Natal, 2020 79.

Access by law enforcement officials to the records stored by electronic communications service providers is controlled under the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA).⁶⁰ Nothing in the regulations is concerned with monitoring communications content,⁶¹ which would remain governed by RICA. However, the regulations supersede the requirements for RICA insofar as they provide for the interception of real-time or archived location data ('communication-related information') without a RICA directive. Under RICA, if only archived communication-related information is required, a magistrate may issue the required directive,⁶² whereas if real-time communication-related information is required on an 'ongoing basis', only a judge of the High Court can issue the directive.⁶³ If another Act makes provision for the interception of communications-related information, such information cannot be collected on an ongoing basis.⁶⁴ There are few exceptions. In situations of urgency, and only in order to prevent serious bodily harm, law enforcement officials can obtain interception of communications or indirect communications without a prior directive, provided that they present an affidavit to a High Court judge as required under RICA as soon as reasonably practicable thereafter.⁶⁵

While the pandemic may have created grounds for extraordinary measures during the suspension of the ordinary democratic process, it is essential to closely scrutinise the national disaster regulations as they have dispensed with the requirement for an interception and monitoring directive and instead authorised the Director-General: Health to issue directives directly to electronic communications service providers to requisition network-based location information.

3.3 Accountability

The Information Regulator's guidance note addressed the question of whether an electronic communications services provider can share 'mobile location-based data of data subjects' with government for the purpose of tracking data subjects.⁶⁶ The question appears to be directed to the tracking

60 Act 70 of 2002.

61 Regulation 11H (12) provides: 'Nothing in this regulation entitles the Director-General: Health or any other person to intercept the contents of any electronic communication.'

62 RICA sec 19(1). These provisions are preserved by sec 40(2) of the Cybercrimes Act 19 of 2020.

63 RICA sec 17(1).

64 RICA sec 15(2).

65 RICA secs 7(1) & (2).

66 Information Regulator (n 37) para 5.1.

of an identifiable data subject, and reference to 'mobile location-based data' probably refers to the provision of network-based location data by electronic communications services providers, but could include location tracking by mobile applications. In this context, it must be assumed that the location data has not been de-identified and must be processed in full compliance with POPIA.

A responsible party is defined under section 1 of POPIA as 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'. Thus, each entity that collected personal information would be regarded as a responsible party. In addition, the National Department of Health, as the recipient of the location information, is a responsible party in respect of its storage of the data in the COVID-19 tracing database and its use of the data for monitoring COVID-19. As such, the Director-General: Health must ensure compliance with all eight conditions of lawful processing for the entire lifecycle of the data (from receipt until destruction or de-identification of the data).

3.4 Processing limitation: Lawful justification

Any collection and transfer of personal information by collection and testing sites and electronic communications services provider to the Director General: Health falls within the definition of 'processing' under POPIA and, as such, requires a lawful justification under section 11 of the Act. While consent of the data subject is the first basis for lawful processing, it is not the only permitted ground. As the regulations imposed duties upon all persons collecting and testing samples to collect and transfer the information they would, as responsible parties under POPIA, be able to rely on subsection 11(1)(c) in that 'processing complies with an obligation imposed by law on the responsible party'. The data subject has no right to object to such processing.⁶⁷ The processing by public bodies such as the National Department of Health could also be justified under subsection 11(1)(e) which provides for processing that 'is necessary for the proper performance of a public law duty by a public body'. Processing could also be justified as being in the legitimate interests of the National Department of Health, as the party receiving the data,⁶⁸ or even in the

67 POPIA sec 11(3)(a) provides: 'A data subject may object, at any time, to the processing of personal information (a) in terms of subsection (1)(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, *unless legislation provides for such processing*'.

68 POPIA sec 11(1)(d).

‘legitimate interests of the data subject’ to know if they have contracted or been exposed to COVID-19.⁶⁹

However, POPIA does not simply require a lawful justification for processing. It also imposes a requirement that processing should be reasonable and respect the data subject’s privacy.

3.5 Reasonableness and the right to privacy

Section 9 of POPIA requires that all processing must be undertaken ‘in a reasonable manner that does not infringe the privacy of the data subject’.⁷⁰ In general, the disclosure of a person’s identity might constitute a breach of the right to privacy in certain circumstances.⁷¹ Not all personal information will be the kind of private facts and private documents that enjoy protection under the right to privacy.⁷² However, the data being collected for the COVID-19 tracing database clearly is private information and must be accordingly handled with appropriate safeguards.

An individual’s medical records, such as the results of a COVID-19 test being entered in the COVID-19 tracing database, are sensitive and personal information that is private and confidential.⁷³ Disclosure is ordinarily strictly regulated by the National Health Act.⁷⁴ Where disclosure takes place in accordance with law, our courts have found that there is no invasion of privacy and no breach of POPIA,⁷⁵ but such cases require careful attention to the constitutionality of the law and whether it has been complied with.⁷⁶

69 POPIA sec 11(1)(b).

70 POPIA sec 9(b).

71 *Bernstein & Others v Bester & Others* NNO 1996 (2) SA 751 (CC) para 58. The Court provides an extensive discussion of the right to privacy from para 65 onwards.

72 Constitution of the Republic of South Africa 1996, sec 14.

73 *Tshabalala-Msimang & Another v Makhanya & Others* 2008 (6) SA 102 (W) para 26 onwards.

74 Act 61 of 2003 sec 14, which will be applied together with any applicable law relating to discovery or compulsion of evidence in civil and criminal proceedings. See *Unitas Hospital v Van Wyk & Another* 2006 (4) SA 436 (SCA) para 21; *Industrial Development Corporation of South Africa Ltd v PFE International Inc (BVI) & Others* 2012 (2) SA 269 (SCA) 275B-C.

75 *Divine Inspiration Trading 205 (Pty) Ltd & Another v Gordon & Others* 2021 (4) SA 206 (WCC).

76 This chapter will not conduct an analysis of the constitutionality of the regulations. The unfortunate judgment in *De Beer & Others v Minister of Cooperative Governance and Traditional Affairs* 2020 (11) BCLR 1349 (GP) was swiftly set aside in *Minister of Cooperative Governance and Traditional Affairs v De Beer & Another* [2021] 3 All SA 723 (SCA), with the SCA cautioning at para 2 that any constitutional challenge should be approached in a disciplined and cautious manner.

The location information being collected for the COVID-19 tracing database must also be treated as private. Evidence presented in the case of *Carpenter v United States*⁷⁷ revealed just how privacy-invasive such digital shadowing can be. Authorities had collected 12 898 time-stamped location points recording Carpenter's movements over 127 days – an average of 101 data points per day. The United States Supreme Court found that this was a clear invasion of privacy as it creates an 'intimate window' into an individual's life, 'revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations"''.⁷⁸

As such, the regulations pertaining to the COVID-19 database must be carefully analysed to determine whether they provide for full compliance with all conditions for lawful processing, or whether their implementation would result in an infringement of privacy that will *ipso facto* be unreasonable for the purposes of section 9 of POPIA.

3.6 Minimality

The processing limitation and reasonableness requirement are further embodied in the principle of 'minimality'. POPIA provides that '[p]ersonal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive'.⁷⁹ In this regard the regulations fall short.

Viljoen and others note that since network-based location information cannot identify a close contact (as it does not have the pinpoint accuracy of GPS location information) the use of such a 'technically inappropriate method [is] questionable'.⁸⁰ On this basis I would argue that the adequacy and relevance of the location data for the specified purpose have not been made out.

Furthermore, the scope of data collection is potentially excessive. The regulations stipulate that such information can only be requested 'during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated'.⁸¹ However, what is absent from the regulations is any indication of the time frame for which location data can be collected about a particular individual. On the face of it, the Director-

77 *Carpenter* (n 57) 3.

78 *Carpenter* (n 57) 12, citing *United States v Jones* 565 US 400 415.

79 POPIA sec 10.

80 Viljoen and others (n 25) 21.

81 Regulation 11H (11)(a).

General: Health may direct electronic communication service providers to transfer mobile-location data on every person whose details were collected under the regulation on an ongoing basis throughout the national state of disaster.

To be lawful in terms of their own stated purpose, however, the regulations must be interpreted as impliedly limiting the collection of such data to specific persons whose contacts needed to be traced, and for a limited period that could be scientifically justified as necessary for contact tracing. This would mean that mobile-location data could only be relevant to contact tracing in relation to a person after a positive test result was confirmed for that person and in instances where there was no other reliable information about that person's current location, or about their contacts during the period they were known or suspected to have been infectious. Given that the Regulations appear to authorise the Director-General: Health to requisition the details of any person who was tested (even before the result of their test was known)⁸² and all their reported known or suspected contacts, a further implied limitation should be read in that the information obtained will not be entered automatically into the COVID-19 tracing database. If the test result is subsequently negative, or if reliable contact details have been provided, the data should be deleted.

It follows that to comply with the minimality principle, only historical mobile-location for a reasonable number of days prior to testing during which the person may have been infectious could be justified. To ensure compliance with the principles of lawfulness, transparency and data subject participation the regulations ought to have specified this period.

The regulations do not do this, referring widely to 'the location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated, with a person contemplated in subparagraph (a)'.⁸³

Clearly, on face value this cannot be interpreted as permitting ongoing location tracking of any single individual for the entire period. Ongoing monitoring of the location of an individual would be a clear invasion of privacy that would be grossly disproportionate to the lawful object of the

82 Regulation 11H(10)(a) refers to 'the location or movements of any person known or *reasonably suspected* to have contracted COVID-19'. The determination that there is a known or reasonably suspected case of COVID-19 is made by the DG Health, but must be objectively reasonable on a sound scientific basis..

83 Regulation 11H(10)(b).

regulations, and never justifiable when one considers the stated purpose of the regulations.

3.7 Purpose specification

POPIA requires that any responsible party processing data must have 'a specific, explicitly defined and lawful purpose' for collecting the data,⁸⁴ and this purpose then acts as a brake on further processing, which must always be compatible with the original purpose of collection, unless a new ground of justification can be established.⁸⁵

The regulations' stated purpose for the processing of mobile location data was clearly expressed. The information 'may only be obtained, used and disclosed when necessary for the purposes of addressing, preventing or combatting the spread of COVID-19 *through the contact tracing process*'.⁸⁶ This is a significant safeguard protecting against 'function creep', where data is used for a purpose for which it was not originally collected.⁸⁷ It is clear from the regulations that they do not permit transfer of the data collected for the COVID-19 tracing database to other government departments, such as the police,⁸⁸ or to private bodies, such as employers.⁸⁹

The regulations ought to have also contained a specific indication of whether any mobile-location data could be collected about an individual after their positive test result, and if so this should have been limited to the number of days they were likely to remain infectious. Even if the regulations had contained such a limitation the rationale for such collection would be much weaker, as a person who has tested positive would be self-isolating or in a quarantine facility. The regulations were expressly limited to what was necessary for *contact tracing*, and did not authorise the collection of information to monitor quarantine compliance.

84 POPIA sec 13(1).

85 POPIA sec 15(1).

86 Regulation 11H (11)(b) (my emphasis).

87 Bradford (n 24) 11.

88 N Sun and others 'Human rights and digital health technologies' (2020) 22 *Health and Human Rights Journal* [special section 'Big Data, Technology, Artificial Intelligence and the Right to Health'] 22.

89 As to the position of employees generally, see DT Hagemester and others "'Please confirm your HIV-positive status by email to the following government address": Protection of "vulnerable employees" under COVID-19' (2020) 13 *South African Journal of Bioethics and Law* 91.

Moreover, ongoing monitoring of location data for an unspecified period would, I argue, never be justified.

3.8 Storage limitation

POPIA provides that ‘records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed’.⁹⁰ Although POPIA contains an exception where ‘retention of the record is required or authorised by law’ or when ‘the responsible party reasonably requires the record for lawful purposes related to its functions or activities’,⁹¹ these would still be subject to the requirement of reasonableness in section 9.

The regulations provide two different storage limitations. First, data not included in the COVID-19 tracing database ‘may only be retained by the Director-General: Health for a period of six weeks after being obtained and shall thereafter be destroyed’.⁹² However, this limitation will not apply in many cases, as mobile-location data ‘where relevant to the contact tracing process, must be included in the COVID-19 tracing database’.⁹³ Data in the database will be retained in a personally-identifiable form until the end of the national state of disaster, after which it must be de-identified within six weeks.⁹⁴

If the data has been de-identified, it will no longer be personal information, and it ‘shall be retained and used only for research, study and teaching purposes’.⁹⁵ As de-identified data is no longer subject to POPIA, it can be retained indefinitely. If it is not de-identified, it will be destroyed.⁹⁶ Given the importance of protecting privacy, it is welcome that the regulations contain a restriction on the purpose for which de-identified data may be used, although the scope of such purpose remains broad. It is further welcome that the measures taken must be reported to the COVID-19 judge. However, it is to be hoped that the judge recommends scrutiny of the data by a professional qualified to determine whether the data has been de-identified and that there is no reasonable risk that it could be reconstructed or linked with other data to re-identify individuals. Collection of mobile location data on a large scale or for an extended

90 POPIA sec 14(1).

91 POPIA secs 14(1)(a) & (b).

92 Regulation 11H (11)(d).

93 Regulation 11H (11)(c).

94 Regulation 11H (17)(a).

95 Regulation 11H (17)(b).

96 Regulation 11H (17)(c).

period, even if it will subsequently be anonymised, would not meet the conditions for lawful processing under POPIA.

3.9 'Anonymous' mass surveillance

The Regulator's guidance note addressed a second question, namely, whether an electronic communications service provider can share location-based data with the government 'for the purpose of conducting mass surveillance of data subjects' in its COVID-19 response.⁹⁷ Here the Regulator's position was that this is only permissible 'if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form'.⁹⁸

The recommendation lacked any teeth since POPIA only became binding on 1 July 2021 but, more to the point, it should have raised alarm bells about whether, and by what means, 'mass surveillance' was taking place when (as set out above) such measures were not contained within the purpose of the regulations as framed. Second, it should have fully addressed what is required for de-identification of data.

Truly de-identified data serves no purpose for contact tracing – the stated purpose of the regulations. Although governments around the world conceived large-scale monitoring of aggregated location data as helpful for modelling the spread of the virus and thus assessing the effectiveness of lockdown restrictions in slowing or containing the pandemic,⁹⁹ these aims were not addressed in the regulation's stated purpose. Thus, no matter how useful this information may be, the regulations did not permit its collection, even in an anonymous form.

Second, to regard data as anonymous a strict test must be applied. Anonymisation, or de-identification as it is termed in POPIA, refers to the principle that data is de-identified when it cannot directly or indirectly identify an individual. There must be 'no reasonably foreseeable means of reversing the de-identification (re-identifying the information), or linking the information to other information and in that way identifying the data subject'.¹⁰⁰ This principle is expressed in slightly different but consistent

97 Guidance note (n 37) para 5.2.

98 As above.

99 European Data Protection Board (n 6) 5 recommended that preference always be given to anonymised data over personal data.

100 Donnelly (n 59) 79.

ways in most data protection statutes around the world.¹⁰¹ These include Recital 26 of the General Data Protection Regulation 2016/679 (GDPR) in the European Union (EU)¹⁰² and section 164.514 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA privacy rule) in the United States.¹⁰³

The critical attribute of de-identified data is not only that it has been irreversibly stripped of direct identifiers but that there is no reasonable possibility that an individual can be re-identified by manipulating the data or linking it to other data. As the European Data Protection Board has explained, reasonableness in this context refers to both general objective criteria such as the currently available technology and time required for re-identification, and to the specific circumstances of a particular case where, for example, the rarity of a phenomenon or scarcity of data may make it more likely that a particular individual can be identified.¹⁰⁴

A growing body of research has shown that re-identification attacks can be performed with relative ease and that mobile location data is particularly vulnerable owing to the uniqueness of an individual's 'mobility traces'.¹⁰⁵ For example, anonymised location data with four spatio-temporal points can identify 95 per cent of individuals from their pattern of movements,¹⁰⁶ and one study showed that 99.9 per cent of individuals in the state of Massachusetts could be correctly re-identified from an anonymised dataset containing only 15 demographic variables.¹⁰⁷

This means that the protection offered by an assurance that data will be de-identified is highly dependent on the techniques used to anonymise the data. POPIA, being technologically neutral principles-based legislation,

101 L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117 *South African Journal of Science* 1.

102 General Data Protection Regulation: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016.

103 Health Insurance Portability and Accountability Act of 1996 PubL 104–191; 110 Stat 1936.

104 European Data Protection Board (n 6) 5.

105 As above.

106 Y de Montjoye and others 'Unique in the crowd: The privacy bounds of human mobility' (2013) 3 *Scientific Reports* 1.

107 L Rocher and others 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) 10 *Nature Communications* 5.

does not specify any particular anonymisation technique. However, there is no reason why the regulations, if they intended to authorise the collection of aggregated location data, should not have set out both the requirement for it to be de-identified, as well as steps to be taken by the electronic communications service provider to confirm that the data was de-identified before it was transferred.

The danger of referring to data as anonymous is that it then falls outside the ambit of POPIA. Too ready reliance on anonymisation as a safeguard could lead governments to act with impunity and disregard POPIA altogether in the belief that the Act does not cover the data. Given the difficulty of genuinely anonymising data, it should rather be treated as pseudonymised and then handled subject to POPIA with due regard for the data subject's right to privacy and the obligations to ensure the security and integrity of the data.

3.10 Security

The regulations outline, in broad strokes, the protection of the confidentiality of the data collected.¹⁰⁸ If those assurances are to offer solace, they must be operationalised by technical and organisational measures to limit access to the data to authorised persons only and guard against loss, damage, or unauthorised destruction of the data.¹⁰⁹ The servers on which it is stored, the devices on which it is accessed, and the applications or networks through which it is transmitted must all be secure,¹¹⁰ and measures must be in place to ensure that unauthorised access to data is swiftly detected and that data breaches are promptly reported.¹¹¹ While it may be sufficient to detail such measures in internal policies and procedures and not in the regulations themselves, the lingering concern remains that 'not enough

108 Regulation 11H (11) provided that the location data referred to in sub-regulation (10) 'may only be obtained, used or disclosed by authorised persons'. Further sub-regulation (4) stipulated that all information in the COVID-19 tracing database or obtained under the regulations is confidential. In terms of sub-regulation (5): 'No person may disclose any information contained in the COVID-19 tracing database or any information obtained through this regulation unless authorized to do so and unless the disclosure is necessary for the purpose of addressing, preventing or combatting the spread of COVID-19.'

109 POPIA sec 19(1).

110 Viljoen and others (note 25) 23.

111 POPIA sec 22 read with sec 19(2) which requires ongoing monitoring to verify that safeguards have been implemented effectively, and sec 19(4).

attention has been given to exactly how confidentiality is protected, and what will happen if it is breached'.¹¹²

3.11 Openness and data subject participation

Even when consent is not relied upon as the legal justification for processing, the principle of openness requires that the data subject should ordinarily be notified about the processing.¹¹³ Notice to the data subject should also inform them of any necessary information to render the processing reasonable, including informing them of their right of access to the data records held on them, and their right to rectify the information in those records.¹¹⁴ It follows that the responsible party must make it possible for the data subject to exercise these rights. Under POPIA, non-compliance with section 18 is condoned only on reasonable grounds, including where 'compliance is not reasonably practicable in the circumstances of the particular case'.¹¹⁵

Under the regulations the Director-General: Health is authorised to requisition the information without prior notice to the persons concerned.¹¹⁶ The regulations provide that every person whose information is obtained will be notified 'within six weeks after the national state of disaster has lapsed',¹¹⁷ but there is no provision for access to or rectification of the data.

Electronic communications service providers were required to 'promptly comply' with any written directive from the Director-General. No appeal mechanism was created. Non-compliance is an offence for which a person is liable, on conviction, to a fine or imprisonment for up to six months, or both such fine and imprisonment.¹¹⁸

The regulations contain a significant safeguard for the constitutional right to privacy. Retired Constitutional Court Justice O'Regan was appointed¹¹⁹ to receive weekly reports providing the names and details of all persons whose location and movements were obtained by the

112 Viljoen and others (n 25) 24.

113 POPIA sec 18(1).

114 POPIA sec 18(1)(h)(iii).

115 POPIA sec 18(4)(e).

116 Regulation 11H (10).

117 Regulation 11H (16).

118 Regulation 11I.

119 Regulation 11H (13), read with Government of South Africa 'Media statement' 4 April 2020, <https://www.sanews.gov.za/south-africa/o%E2%80%99regan-appointed-covid-19-designated-judge> (accessed 11 October 2021).

Director-General: Health.¹²⁰ The judge has the power to make such recommendations as she deems fit 'regarding the amendment or enforcement of this regulation in order to safeguard the right to privacy while ensuring the ability of the Department of Health to engage in urgent and effective contact tracing to address, prevent and combat the spread of COVID-19'. However, it does not appear that she has done so. She will also receive a final report that confirms the steps taken to notify every person whose location data was collected about that fact and the steps taken to destroy or de-identify the data,¹²¹ and she may give directions as to any further steps that must be taken to safeguard the right to privacy.¹²² Both the report and any directions given by the judge will be tabled in Parliament.¹²³ While the provision seems reasonable on the face of it, the longer the national state of disaster persists, the weaker the rationale becomes for not complying fully with POPIA.

4 Location monitoring and the public interest exemption

In view of the analysis that the regulations do not comply with POPIA it must be considered whether that non-compliance meets the grounds for an exemption. Although the power was not exercised during the COVID-19 pandemic, section 37(1) of POPIA empowers the Information Regulator to exempt a responsible party from compliance with a condition of lawful processing, in cases where:

- (a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or
- (b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

The concept of public interest is a broad one that defies attempts at a precise or comprehensive definition.¹²⁴ Its core component is that the action should benefit the public by improving public welfare or services. On a narrow view, it suffices if the public at large can be said to enjoy

120 Regulation 11H (14).

121 Regulation 11H (17)(d).

122 Regulation 11H (18).

123 Regulation 11H (19).

124 *Rail Commuter Action Group & Others v Transnet Ltd t/a Metrorail & Others (No 1)* 2003 (5) SA 518 (C) 558A-B, and *Argus Printing and Publishing Co Ltd v Darbys Artware (Pty) Ltd* 1952 (2) SA 1 (C) 8-10.

the general benefit contemplated in the empowering legislation.¹²⁵ On a broad view, it means only that ‘the public would be better off by having the service than by being without it’.¹²⁶ While the concept generally refers to the public at large, as opposed to a few or even a single person or entity,¹²⁷ in certain circumstances, the ‘public’ might properly refer only to a specific group or community.¹²⁸

Context matters. The Constitutional Court has held:¹²⁹

Determining the scope of public power, therefore, and any duties attached to it requires an analysis not only of the statutory provisions conferring the power, but also of the social, political and economic context within which the power is to be exercised and a consideration of the relevant provisions of the Constitution. If this approach is followed, the ambit of public duties of organs of state will be drawn in an incremental and context-driven manner.

Thus, the Court’s determination of the public interest will always be made on a consideration of the facts as a whole. There may be instances where there are potentially competing public interests, such as where a particular group stands to benefit, but there could be adverse consequences for other groups or the public more generally. Thus, all consequences of the processing (positive and negative) must be considered and given appropriate weight.¹³⁰

125 Eg, in *Transnet Ltd t/a Metrorail & Others v Rail Commuters Action Group & Others* 2003 (6) SA 349 (SCA) para 17, per Howie P and Cloete JA, it was held to be sufficient that Metrorail provided transport services and the concept of ‘public interest’ did not impose any duties in relation to the safety or security of rail commuters.

126 *Transnet v Rail Commuters Action Group* (n 116) minority judgment of Streicher JA para 2.

127 Information Regulator of South Africa ‘Guidance note on exemptions from the conditions for lawful processing of personal information in terms of section 37 and 38 of the Protection of Personal Information Act 4 of 2013’ June 2021 para 4.2.3.3, <https://justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf> (accessed 17 October 2021).

128 See eg *Asko Beleggings v Voorsitter van die Drankraad NO* 1997 (2) SA 57 (NC) 66H and 67E/F-F where the enquiry was whether the granting of a liquor store licence was in the interests of the residents of the town. Also see *Maharaj v Chairman, Liquor Board* 1997 (1) SA 273 (N).

129 Fittingly, the unanimous judgment of the Constitutional Court was penned by O’Regan J, the current designated COVID-19 judge. See *Rail Commuters Action Group & Others v Transnet Ltd t/a Metrorail & Others* 2005 (2) SA 359 (CC) para 85.

130 *Transnet v Rail Commuters Action Group* (n 116) 376B, approving *Clinical Centre (Pty) Ltd v Holdgates Motor Co (Pty) Ltd* 1948 (4) SA 480 (W) 489.

In a general sense, the COVID-19 monitoring and contact-tracing measures can be said to be in the public interest. That alone does not suffice. It must also be shown that the public interest in processing 'outweighs, to a *substantial degree*, any interference with the privacy of the data subject that could result ...'¹³¹ The concept of public interest thus is not an easy threshold to meet and will not exonerate responsible parties from incorporating protections for the privacy of personal information wherever this is reasonably possible.

As the capacity to collect and analyse digital data grows, sharp contests may be anticipated around the use of personal information by public and private entities alike. Similarly, contests will arise around access to information and freedom of expression, particularly media freedoms, where a distinction must be drawn between reporting in the public interest and reporting what is of mere interest to the public.¹³² The concept of public interest may also shape the measures adopted to protect personal information in research.

5 Future COVID-19 research

The rapid development of testing kits and vaccines in the fight against COVID-19 resulted from an enormous collaborative effort within the health research community. Much of this research has necessarily relied upon the collection of personal information and POPIA contains a number of provisions that enable researchers to process personal information.

Processing special personal information such as health data is prohibited unless the data subject has consented to the collection of the data for the intended research purpose¹³³ or, in a research context,¹³⁴ where

processing is for historical, statistical or research purposes to the extent that –

- (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or
- (ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

131 POPIA secs 37(1)(a) & (b).

132 *Centre for Child Law v Media 24 Limited* 2020 (4) SA 319 (CC) para 100.

133 POPIA sec 27(1)(a) read with definition of consent under the Act.

134 POPIA sec 27(1)(d).

The requirements of section 27(1)(d) are less onerous than the requirements for a public interest exemption,¹³⁵ in that the researcher need only show that the effect of the processing is not disproportionately harmful to individual privacy, rather than the more stringent test of whether the public interest purpose of the processing ‘substantially outweighs’ the substantive value of the individual’s privacy interest.

In addition, where another body has collected personal information (with the data subject’s consent, or on another lawful basis) researchers can conduct secondary studies in reliance on the provisions of POPIA that such further processing is deemed compatible with the original purpose where it is for ‘historical, statistical or research purposes’ and ‘will not be published in identifiable form’.¹³⁶

Thaldar and Townsend rightly point out that if the original consent process were flawed, the secondary study would also be tainted.¹³⁷ This caution may apply to research using the proposed de-identified COVID-19 tracing database, if the data was not collected lawfully. On the analysis above, although it was lawful to collect the information without the data subject’s consent, if the extent of the information collected about their location went beyond what was adequate and reasonably required for contact tracing, it should be deleted from the database and not made available to researchers.

It is only if the data was collected in full compliance with POPIA, and if it can be fully de-identified, that it will no longer be subject to POPIA. Nevertheless, even then, given the risk of re-identification, and the fact that the database contains special personal information about the health of individuals (their COVID-19 test results), as well as privacy-sensitive information about their location and movements, research ethics committees should pay careful attention to privacy and security safeguards in the proposed study.

In the case of other repositories of COVID-19 data, the source from which the data or specimens were collected and the justification for that collection will play a key role in determining whether further studies comply with POPIA or require fresh consent from the data subject. The Academy of Science of South Africa is presently facilitating the

135 POPIA sec 37(1) read with sec 37(2)(e) which expressly includes ‘historical, statistical or research activity’ in the meaning of the term ‘public interest’ under POPIA.

136 POPIA sec 15(3)(e).

137 DW Thaldar & BA Townsend ‘Exempting health research from the consent provisions of POPIA’ (2021) 24 *Potchefstroom Electronic Law Journal* 14.

development of a draft code of conduct for researchers, and it is to be hoped that the final code will adequately address this critical issue.

A code can only guide safeguards to comply with POPIA. It cannot amend the definition of consent, which POPIA requires to be informed, voluntary and *specific*.¹³⁸

It follows that where the lawful justification processing was consent, then only narrow consent to a specified research purpose will suffice for processing special personal information such as health data. POPIA does not provide for broad consent, much less blanket consent to future as yet unspecified objectives. Tiered and broad consent may continue to be relied upon for ethical approval of the informed consent process required for all health research in terms of the National Department of Health's research ethics guidelines.¹³⁹ However, in such instances the research proposal would need to contain a different ground to justify processing any personal information collected, such as the public interest grounds set out in section 27 of POPIA.

6 Conclusion

It is vitally important that South Africa harness the power of data in an effective but responsible manner, both for effective governance and impactful evidence-based scientific research. POPIA supports these objectives, and highlights the importance of enabling the free flow of information, provided the personal information and privacy of individuals is protected.

Valuable lessons may be learned from the use of data by the government of South Africa in its response to the COVID-19 pandemic. The starting point for the analysis is that despite the importance of responding effectively and urgently to the pandemic, the right to privacy and the requirements for lawful processing under POPIA must be respected. In this regard the regulations creating the COVID-19 contract-tracing database implemented several important safeguards. Nevertheless, upon scrutiny, more could have been done to comply with the conditions for lawful processing. Before such data is released for research, any data collected outside the lawful bounds of the regulations, read with POPIA,

138 POPIA sec 1.

139 National Department of Health 'Ethics in Health Research Principles, Processes and Structures' 2015 para 3.3.6, <https://www.ul.ac.za/research/application/downloads/DoH%202015%20Ethics%20in%20Health%20Research%20Guidelines.pdf> (accessed 17 October 2021).

must be permanently deleted, and any other personal information must be de-identified to ensure that it is fully and irreversibly anonymised.

References

- Abdool Karim, SS 'The South African response to the pandemic' (2020) 382 *New England Journal of Medicine* e95
- Bates, M 'Tracking disease: Digital epidemiology offers new promise in predicting outbreaks' (2017) 8 *IEEE pulse* 18
- Bengtsson, L, Gaudart, J, Lu, X, Moore, S, Wetter, E, Sallah, K, Rebaudet, & Piarroux, R 'Using mobile phone data to predict the spatial spread of cholera' (2015) 5 *Scientific Reports* 1
- Bradford, L, Aboy, M & Liddell K 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 34
- De Montjoye, YA, Hidalgo, CA, Verleysen, M & Blondel, VD 'Unique in the crowd: The privacy bounds of human mobility' (2013) 3 *Scientific Reports* 1
- Donnelly, D 'Privacy by (re)design: A comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law' PhD thesis, University of KwaZulu-Natal, 2020
- Hagemeister, DT, Mpeli, MR & Shabangu, BE "“Please confirm your HIV-positive status by email to the following government address”: Protection of “vulnerable employees” under COVID-19' (2020) 13 *South African Journal of Bioethics and Law* 91
- Johnson, D 'Assessment of contact tracing options for South Africa' (October 2020) Research ICT Africa Cape Town, <https://researchictafrica.net/wp/wp-content/uploads/2020/10/Contact-tracing-survey-report-David-Johnson-Oct2020.pdf> (accessed 11 October 2021)
- Marcello, I & Vayena, E 'On the responsible use of digital data to tackle the COVID-19 pandemic' (2020) 26 *Nature Medicine* 463
- Mendelson, M & Madhi, S 'South Africa's coronavirus testing strategy is broken and not fit for purpose: It's time for a change' (2020) 110 *South African Medical Journal* 429
- Rocher, L, Hendrickx, JM & De Montjoye, YA 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) 10 *Nature Communications* 1
- Singh, K 'Coronavirus: Authorities pull out all stops, high-level meeting planned with KZN school' 6 March 2020, <https://www.news24.com/news24/SouthAfrica/News/coronavirus-authorities-pull-out-all-stops-high-level-meeting-planned-with-kzn-school-20200306> (accessed 11 October 2021)

- Sun, N, Esom, K, Dhaliwal, M & Amon, JJ 'Human rights and digital health technologies' (2020) 22 *Health and Human Rights Journal* [special section 'Big Data, Technology, Artificial Intelligence and the Right to Health'] 21
- Swales, L 'The Protection of Personal Information Act and data de-identification' (2021) 117 *South African Journal of Science* 1
- Thaldar, DW & Townsend, BA 'Exempting health research from the consent provisions of POPIA' (2021) 24 *Potchefstroom Electronic Law Journal* 1
- Viljoen, IM, De Villebois Castelyn, C, Pope, A, Botes, M & Pepper, MS 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) 13 *South African Journal of Bioethics Law* 20
- Wang, M 'China: Fighting COVID-19 with automated tyranny' *The Diplomat* 1 April 2020, <https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny/> (accessed 18 October 2021)
- Wu, JT, Leung, K & Leung, GM 'Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: A modelling study' (2020) 395.1022 *The Lancet* 689

**PART V: Selected data privacy issues
from a comparative perspective**

11

THE REGULATION OF AUTOMATED DECISION MAKING AND PROFILING IN AN ERA OF BIG DATA AND AMBIENT INTELLIGENCE: A EUROPEAN AND SOUTH AFRICAN PERSPECTIVE

Alon Lev Alkalay

Abstract

The twenty-first century presents a challenge to human liberties as automated decision-making (ADM) and profiling technologies advance. Enabled by big data (BD) and machine learning (ML), these technologies delve into ‘invisible knowledge,’ with the capability to manipulate human emotions and behaviours. The looming era of ambient intelligence (AmI) amplifies these concerns by seamlessly integrating computing and biometric technologies into environments. Regulatory efforts such as the GDPR and POPIA signal recognition of these challenges but fall short in addressing evolving technological landscapes. This chapter scrutinises EU and South African data protection laws, assessing their adequacy in the face of ADM and profiling in BD and AmI contexts. Through conceptual analysis and comparison, it aims to illuminate regulatory shortcomings and propose pathways for governance in an era defined by algorithmic influence.

1 Introduction

Whether or not we are conscious of (or care to acknowledge) it, humans are organisms, ‘organisms are algorithms’¹, and algorithms can be ‘hacked’.² On this note, two pervasive technological developments – and the technical processes of automated decision making (ADM) and profiling that they facilitate – will pose a challenge to the assurance of human liberties in the twenty-first century. Today, the confluence of a data-driven information society; exponentially increasing levels of processing power; limitless cloud storage and ML algorithms have resulted in an era of big data (BD).³

1 See YN Harari *Homo Deus: A brief history of tomorrow* (2016) 383. See also YN Harari *21 Lessons for the 21st Century* (2018) 47.

2 ‘Hacked’ in this instance refers to unauthorised access to the inner workings of the human mind and body.

3 ‘Big data’ may be understood as ‘novel ways in which organi[s]ations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations’. See IS Rubenstein ‘Big data: The end of privacy or a new beginning?’ (2013) 3 *International Data Privacy Law* 74.

Thereunder, the abilities to (i) make automated decisions concerning humans; and (ii) manipulate human emotions, perceptions, behaviours, preferences and habits, are being fostered by entities that are learning to know us better than we understand ourselves as a result of the extraction and utilisation of ‘invisible knowledge’⁴ hidden within large sets of data. We are, after all, algorithms at our core.

Tomorrow, an era of ambient intelligence (AmI)⁵ has been envisioned⁶ that will build upon BD processing by injecting a combination of autonomic, omnipresent computing⁷ and ‘second generation’⁸ biometric technologies into smart, sensor-rich environments that are ‘capable of recognising and responding to individuals in a seamless, unobtrusive and invisible way’⁹ by preemptively adapting to human preferences.¹⁰ Hildebrandt and Koops describe these intelligent environments as being akin to ‘digital butler[s]’.¹¹

Whereas BD has already facilitated automated decision making (ADM) capabilities and profiling practices, an era of AmI – despite having the potential to positively impact many aspects of life – will elevate and proliferate these processes and broaden their potential impact on fundamental human liberties as a result of unseeable ‘prejudicial computations’.¹² Consequentially, the regulation of automated processes – which has already begun in the European Union (EU) under its General

4 See M Hildebrandt ‘Who is profiling who? Invisible invisibility’ in S Gutwirth and others (eds) *Reinventing data protection?* (2009) 239.

5 M Hildebrandt ‘Profiling and AmI’ in K Rannenberg, D Royer & A Deuker (eds) *The future of identity in the information society: Challenges and opportunities* (2009) 286.

6 AmI is a European conceptualisation by the European Information Society Technologies Advisory Group (ISTAG). In other parts of the world, similar conceptualisations take the form of ‘ubiquitous computing’ (United States of America) and ‘ubiquitous networking’ (Japan), for example. See SE Bibri *The shaping of ambient intelligence and the internet of things* (2015) 89.

7 Hildebrandt (n 5) 288.

8 Instead of identifying ‘who you are’, second generation biometrics focus on determining ‘how you are’ in relation to your environment. For a detailed investigation into second generation biometrics, see E Mordini & D Tzovaras (eds) *Second generation biometrics: The ethical, legal and social context* (2012) 11.

9 D Wright, S Gutwirth & M Friedewald (eds) *Safeguards in a world of ambient intelligence* (2008) 1.

10 M Hildebrandt & B-J Koops ‘The challenges of ambient law and legal protection in the profiling era’ (2010) 73 *Modern Law Review* 431.

11 As above.

12 The phrase ‘prejudicial computations’ is used here to refer to mathematical and statistical outcomes, inferences or decisions that are either used to create/apply a profile, or make an automated decision in regard to a data subject.

Data Protection Regulations 2016/679 (GDPR)¹³ and in South Africa under its Protection of Personal Information Act 4 of 2013 (POPIA)¹⁴ – has become a topic of increasing discussion among academia and policy makers abroad, signifying the relevance of contributing to, and continuing this discussion within a South African context.

Considering the foregoing, in this chapter¹⁵ I will seek to explore the extent of EU and South African data protection laws and their adequacy in light of the ethical and legal issues that may arise from ADM and profiling practices in an era of BD and AmI. Ultimately, I will aim to highlight that despite recent overhauls, the current state of data-protection law – utilising the EU and South Africa as jurisdictional yardsticks – contains fundamental flaws that significantly impact on its adequacy in an era of BD and AmI.

This chapter is divided in five parts. I begin the exploration in part 2 by conceptualising and differentiating ADM and profiling to enable a proper analysis of the laws under consideration. Thereafter, in part 3 I unpack and compare the definitions, semantics, and provisions of GDPR and POPIA in order to assess the extent of their regulative postures towards ADM and profiling. In part 4 I consider the adequacy of these laws today (in the context of BD), and tomorrow (in the context of AmI) and thereafter collate and build upon recommendations that have been posited for the future regulation of ADM and profiling. Finally, in part 5 I provide concluding remarks as to the findings of the exploration undertaken through this chapter.

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

14 Protection of Personal Information Act 4 of 2013 (POPIA).

15 I note two limitations to the scope of this chapter. First, the chapter will exclusively concern itself with solely automated ADM and profiling practices, conducted by non-state entities (with an emphasis on corporations). Second, while it is acknowledged that ADM and profiling technologies may be subject to constitutional scrutiny, the chapter primarily focuses on the extent and adequacy of laws provided at a statutory level – specifically in regard to GDPR and POPIA. Accordingly, the manner in which consumer protection, anti-discrimination and equality, and artificial intelligence laws eg, may impact ADM and profiling practices, will not be considered herein. Finally, I acknowledge that specific terminological differences exist between GDPR and POPIA. Having said that, throughout this chapter I shall primarily make use of terminology contained in POPIA, except where I am specifically discussing GDPR.

2 Conceptualising and differentiating automated decision making from profiling

In order to properly explore the extent and adequacy of the current regulation of ADM and profiling, one must understand the manner in which these technological processes function and relate with one another. Accordingly, before conceptualising ADM and profiling in their own right, I wish to note three over-arching dynamics that bear an impact on the regulation of these processes – all of which will be canvassed more fully across parts 3 and 4.

First, despite being distinct processes that may take place independently, ADM and profiling are often interrelated. In many instances, decisions are reached by applying profiles, while profiles may also be constructed by considering a set of automated decisions – they may, therefore, feed into one another.

Second, both ADM and profiling may, or may not (where human control is involved) be solely automated – resultantly, EU and South African legislators have adopted what I regard as a ‘two-prong approach’ to these processes, so as to regulate solely automated instances and those including human involvement, separately.

Third, both ADM and profiling may, or may not, involve the processing of ‘personal information’. Where ‘group profiles’ or ‘de-identified’ personal information are involved, a significant lacuna arises in the laws under consideration.¹⁶

2.1 Automated decision making

In its simplest form, ADM may be regarded as the arrival at a decision by a computer system, made autonomously, without human involvement.¹⁷ Logically, for a decision to be made autonomously, it must be based upon data, which may be either (i) collected; (ii) observed; or (iii) inferred.¹⁸ The

16 S Gutwirth & P de Hert ‘Regulating profiling in a democratic constitutional state’ in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008) 288.

17 Art 29 Data Protection Working Party (251rev.01) *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (2017) 8.

18 As above.

various sources of data that ADM can be based upon the application of profiles but need not necessarily be.¹⁹

2.2 Profiling

‘Profiling’ is not a concept isolated to the realms of information technology. In fact, humans and animals profile the world every day.²⁰ However, insofar as this chapter is concerned – and the laws that I seek to explore – I posit a working definition of ‘profiling’ as ‘the process of using algorithms to *construct* “probabilistic knowledge” (inferences/predictions) through the discovery of correlations in large datasets, which knowledge may be *applied* by identifying, representing or making decisions about, an individual or group of data subjects’.²¹

For the sake of clarity, I will extrapolate two core elements from the above working definition. First, profiles can be both ‘constructed’ (inferred from data) and ‘applied’ (through identification, representation or in the course of decision making).²² Second, any construction or application of a profile can be carried out both ‘individually’ (upon specific data subjects) as well as ‘collectively’ (upon groups of anonymous data subjects – ‘group data’).²³ Further, their application can be direct (upon the same data subject to whom the profile relates) or indirect (where a profile from another person or group is applied to the data subject).²⁴ Importantly, when profiles are applied, new profiles may be created that may then enter a feedback loop of profile application and profile creation to ‘mine’ further ‘knowledge’. The legal issues relating to indirect ‘group profiling’ will be clarified in part 4.

19 Example: A driver receives a traffic fine for speeding measured by an average-speed-over-distance camera. In this instance, the mere evidence that the driver sped resulted in an automated decision about the driver’s road conduct. No profile was applied when reaching the automated decision. Yet, it is plausible that a system may assess a driver’s conduct over time (creation of a profile), which profile may then be applied (either manually or autonomously) when determining the quantum of the driver’s fine.

20 M Hildebrandt ‘Defining profiling: A new type of knowledge’ in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008) 25-27.

21 Hildebrandt (n 21) 19 (my emphasis).

22 Hildebrandt (n 21) 18.

23 Hildebrandt (n 21) 20-21.

24 Hildebrandt (n 21) 34-35.

As eluded to above, in practice the lines between decision making and profiling can blur, which has led some legal scholars to perceive the profiling process more broadly as including the making of decisions.²⁵ While profiles may be applied during decision making, this is not their only function – for example, profiles may be created and applied to other profiles when identifying or representing data subjects or a group. Accordingly, the making of a decision based on a profile is a separate activity that falls within the domain of decision making or ADM. In the former case, profiling is an algorithmic process to find new ‘knowledge’ and uncover ‘patterns’ or ‘correlations’, whereas in the latter case, the application of a profile for decision making is not.

3 Exploring the extent of regulation under GDPR and POPIA

3.1 Primary legal instruments

3.1.1 European Union

Statutory protection against the unlawful processing of personal data – which implicitly includes unlawful ADM and profiling practices – is principally rooted in article 8 of the Charter of Fundamental Human Rights of the European Union 2009,²⁶ titled ‘protection of personal data’. Interestingly, the regulation of ADM had been considered by EU legislators 14 years prior under article 15 of the Data Protection Directive (DPD).²⁷ However, as Savin puts it, the provisions contained in the DPD, ‘although introduced in a technically neutral manner, [were] in need of modernisation’.²⁸

In response, a set of Regulations were enacted in the form of GDPR. Having been in force since 25 May 2018, GDPR repealed the DPD and standardised data-protection laws across EU member states. Accordingly, GDPR is now the sole regulatory instrument in the EU overseeing ADM and profiling practices. Where controllers engage in unlawful ADM or profiling practices, they may be fined up to 4 per cent of their worldwide

25 See, eg, D Kamarinou, C Millard & J Singh ‘Machine learning with personal data’ in R Leenes, R van Brakel & S Gutwirth (eds) *Data protection and privacy: The age of intelligence machines* (2017) 97.

26 Charter of Fundamental Human Rights of the European Union 2012/C 326/02.

27 Directive 95/46/EC of the European Parliament of 24 October 1995.

28 A Savin ‘Profiling in the present and new EU data protection frameworks’ in PA Nielsen, PK Schmidt & K Dyppel Weber (eds) *Erhvervsretlige emne* (2015) 253.

annual turnover or may be liable for civil damages.²⁹ In terms of article 3, GDPR also has a notoriously vast territorial application – thus in certain instances providing data subjects within the EU with protection against unlawful ADM and profiling practices by foreign controllers.

Before moving on, I wish to stress that while GDPR is a regulation (and therefore binding), the contents of its Recitals are not legally binding and ‘do not have any autonomous legal effect’³⁰ – unlike the operative provisions of its articles. Jurisprudence before the European Court of Justice (ECJ) has confirmed that Recitals do not confer a right,³¹ nor do they restrict a right.³² Saying that, and without deviating into the academic discourse on the purpose of Recitals in EU law,³³ I will, for the analysis that follows below, note two points. First, an EU court will only consider Recitals to ‘dissolve ambiguity’³⁴ – they, therefore, serve a resolutive function and can indirectly shape future law through judicial interpretation. In this regard, until GDPR’s provisions on ADM and profiling come before a European court for interpretation, the operative provisions of GDPR are the primary indicators of the nature and extent of EU regulation. Second, in the context of GDPR (which, as already indicated, is the baseline data protection law for all EU member states), Recitals will serve an important ‘role in transposition’³⁵ when, or if, EU member states codify GDPR’s operative provisions into their respective national laws. Accordingly, in what follows below, I will only refer to relevant Recitals to indicate possible interpretive outcomes that may arise in future case law on the provisions under exploration.

3.1.2 Republic of South Africa

In South Africa, the unjustified collection of personal information about an individual is regarded by its common law as a breach of individual

29 GDPR arts 82 and 83(5), respectively.

30 R Baratta ‘Complexity of EU law in the domestic implementing process’ (2014) 2 *TTPL* 293.

31 *Criminal Proceedings against Nilsson, Hagelgren & Arrborn* (Case C-162/97) 1998 ECR I-07477.

32 *Giuseppe Manfredi v Regione Puglia* (Case C-308/97) 1998 ECR I-7685.

33 An in-depth exploration of the role of recitals in EU law may be found in T Klimas & J Vaiciukaite ‘The law of recitals in European community legislation’ (2008) 15 *ILSA Journal of International & Comparative Law* 61.

34 S Wachter, B Mittelstadt & L Floridi ‘Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation’ (2017) *International Data Privacy Law* 20.

35 *Giuseppe Manfredi* (n 33) 31.

privacy³⁶ – which is broadly protected in section 14 of the Constitution of the Republic of South Africa, 1996. Unlike the EU, the comprehensive protection of personal information under data protection law had only recently been introduced in the form of POPIA, which to a significant extent is predicated on the DPD.³⁷ Under the POPIA, responsible parties may be sanctioned with fines of up to ten million rand for failing to comply with an enforcement notice,³⁸ or civil damages. Notably, POPIA only applies to processing that takes place within the borders of South Africa.³⁹

3.2 What is regulated? Statutory definitions and semantics

3.2.1 GDPR

GDPR governs the processing⁴⁰ and movement of ‘personal data’ by ‘data controllers’⁴¹ which it defines as constituting ‘any information relating to an *identified* or *identifiable* natural person’.⁴² The scope of personal data has not evolved since the DPD,⁴³ and while it may remain broad enough to include ‘any’ information, such information is limited to ‘identifiable’, ‘living’,⁴⁴ ‘natural persons’. Under the same definition, a data subject will be ‘identifiable’ if that data subject can be identified (either directly or indirectly) through an identifier, or by means of ‘factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.⁴⁵ The definition indirectly provides that de-identified personal data, or data relating to a data subject in group data, may be considered ‘personal data’ if it can be re-identified usually through a process of reverse engineering where a data subject can be indirectly identified by combining attributes that may appear to be harmless in

36 See *S v Bailey* 1981 (4) SA 187 W; *O’Keeffe v Argus Printing and Publishing Co Ltd & Another* 1945 (3) SA 244 (C).

37 Y Burns & A Burger-Smidt *A commentary on the Protection of Personal Information Act* (2018) 5-6.

38 POPIA secs 103 and 99, respectively.

39 POPIA sec 3(b).

40 Art 4(2) of GDPR defines ‘processing’ as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’.

41 GDPR art 4(7).

42 GDPR art 4(1) (my emphasis).

43 DPD art 2(a).

44 The definition in art 4(1) does not require that a natural person be ‘living’. However, Recital 27 suggests that the scope of GDPR does not extend to deceased persons.

45 GDPR art 4(1).

isolation.⁴⁶ While in practice the ability of a controller to re-identify would be up to a data subject to prove, I nonetheless view the meaning conveyed in the definition (as it stands) as having potential to safeguard data subject rights in the face of proliferated de-identification practices (more on this in part 4). However, if a dispute were to arise as to the conflict in the definition, a court would seek to clarify the definition in line with the definition's corresponding Recital. On this note, Recital 26 suggests that for a data subject to be identifiable, the process of re-identification must be 'reasonably likely' to be used. If this suggestion were adopted by a court, it would place a further onus on data subjects to prove, objectively, that a controller was likely to re-identify de-identified personal data or group data. In such a case, data subject rights may be inhibited as a result of a heavy evidentiary burden, and it is on this basis that I view the enforceability of the GDPR definition on 'personal data' as potentially being limited in cases of unfair profiling practices.

In respect of ADM and profiling, both processes are recognised as being distinct under GDPR. ADM may be said to be considered implicitly under the definition of 'processing', which relates to 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'.⁴⁷ Conversely, 'profiling' is explicitly defined as 'any form of automated processing of personal data consisting of the use of personal data to *evaluate* certain personal aspects relating to a natural person, in particular to *analyse* or *predict* aspects concerning that natural [person]'.⁴⁸ (emphasis added).

3.2.2 POPIA

The POPIA adopts a slightly nuanced approach to that of the GDPR regarding its semantics. The POPIA applies to all 'processing'⁴⁹ of personal information which it defines as 'information relating to an *identifiable, living, natural* person, and where it is applicable, an *identifiable, existing juristic* person'.⁵⁰ The definition also includes a widening mechanism under which a non-exhaustive range of personal information may be protected. Unlike GDPR, POPIA does not go on to define what 'identifiable' means in the context of its definition of personal information, or whether the term

46 Contrary to popular belief, re-identification of de-identified data is possible, especially when machine learning algorithms are involved. See Hildebrandt (n 5) 365.

47 GDPR art 4(2).

48 GDPR art 4(4) (my emphasis).

49 Sec 1 of POPIA defines 'processing' as 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information'.

50 POPIA sec 1.

may be understood to include ‘indirect identification’ through a reverse engineering process. Accordingly, until a judicial interpretation takes place, the foregoing indicates that de-identified personal information, or the identity of a data subject in group data, that has been, or is capable of being re-identified, is not protected.

Another notable difference in POPIA’s approach to personal information is that it extends to ‘existing’ juristic persons. This extension of protection is a by-product of South African constitutional and common law that extends the right to privacy to juristic persons.⁵¹ In consequence, under POPIA any rights relating to ADM and profiling apply to juristic persons, which is a welcoming development.

Concerning ADM and profiling, POPIA lacks differentiation of the two processes – an oversight that I will show has caused misinterpretations as to POPIA’s actual regulatory reach. While neither ADM nor profiling is defined, they both fall under the definition of ‘processing’ as ‘any operation or activity or any set of operations, whether or not by automatic means, concerning personal information’.⁵² In fact, the term ‘profiling’ only appears on two occasions throughout the entire Act – both of which merely relate to POPIA’s provisions on ADM.⁵³ Whether or not POPIA regulates profiling will be considered in parts 3.3.2 and 3.3.4 below.

3.3 How is ADM and profiling regulated? The two-prong approach

Native to the architecture of both GDPR and POPIA is a two-prong approach whereby data subjects are afforded varying rights depending on the circumstances surrounding the processing of their personal information. Fundamentally, both laws broadly regulate all forms of processing, on the one hand (prong one), whilst providing specific regulation for instances that are solely automated (no human involvement – prong two), on the other hand – albeit with their own subtleties and nuances. For explanatory purposes, I will categorise the first prong as providing ‘prong one rights’ with the second prong providing ‘prong two rights’. The first prong broadly relates to all forms of processing of personal information – including ADM and profiling – and is best understood as a ‘transparency tool’, which Gutwirth describes as not being prohibitive

51 See *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) and *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A), as read with sec 8(4) of the Constitution of the Republic of South Africa, 1996.

52 POPIA sec 1.

53 POPIA sec 5(g) as read with sec 71(1).

but '[aimed] at channelling, regulating and controlling'⁵⁴ the processing of personal data in an acceptable, fair manner. Structurally, I view and will address this prong as comprising three elements that seek to instil accountability⁵⁵ in responsible parties. These elements are (i) processing principles/conditions;⁵⁶ (ii) grounds for lawful processing;⁵⁷ and (iii) obligations towards data subjects in respect of any prong one rights they may hold. The second prong exclusively relates to ADM or profiling that is solely automated. Thereunder, over and above 'prong one' rights, data subjects are provided additional 'prong two' rights. Limitations on these prong two rights are also listed, in which case certain 'measures' are required to be put in place by responsible parties to safeguard data subject rights. The second prong is of utmost significance in the context of BD and AmI (more on this in part 4).

Saying that, and before exploring the contents of each prong, I note that a comprehensive discussion of the first prong (which includes the majority of the provisions in GDPR and POPIA) is not possible due to space limitations. While I will provide a complete overview of prong one, I will limit my discussion to the essential aspects therein as they may relate to solely automated ADM and profiling.

3.3.1 *GDPR prong one*

GDPR's first prong provides for processing principles in article 5, lawful grounds for processing in article 6 and data subject rights in articles 12 to 21. The first prong's processing principles require 'accountability'⁵⁸ from controllers who must be able to demonstrate that all processing is (i) lawful, fair and transparent;⁵⁹ (ii) undertaken within the bounds of the original specified, explicit and legitimate purpose for which the data was collected;⁶⁰ and (iii) accurate.⁶¹ In addition, controllers must comply with

54 Gutwirth & De Hert (n 17) 277.

55 See GDPR art 5(2) and POPIA sec 8.

56 POPIA sec 4. For GDPR's principles, see art 5.

57 GDPR arts 6(1)(a)-(f) and POPIA secs 11(1)(a)-(f).

58 GDPR art 5(2).

59 GDPR art 5(1)(a).

60 GDPR art 5(1)(b).

61 GDPR art 5(1)(d).

the principles of ‘data minimisation’,⁶² ‘storage limitation’⁶³ and ‘integrity and confidentiality’.⁶⁴

Beginning with the first and broadest principle, ADM and profiling will be regarded as ‘lawful’ if the processing is predicated on one or more of the following grounds for lawful processing: (i) consent;⁶⁵ (ii) contractual obligations;⁶⁶ (iii) legal obligations;⁶⁷ (iv) vital interests of a data subject;⁶⁸ (v) public interest;⁶⁹ or (vi) the legitimate interests of a controller or those of a third party.⁷⁰

As far as ‘transparency’ is concerned, it is regarded by the European Data Protection Board (EDPB) – previously the Article 29 Working Party (29WP) – as being at the core of GDPR⁷¹ in that it is ‘intrinsically linked to fairness’⁷² and the principle of accountability. I concur with the EDPB in that the enforceability of all data subject rights require transparency between controllers and data subjects. That said, article 12 requires controllers to process ‘transparently’ by (i) communicating with data subjects in a ‘concise, transparent, intelligible and easily accessible form, using clear and plain language’;⁷³ and (ii) facilitating the invocation of prong one rights by enabling and co-operating with data subject requests⁷⁴ – which must be undertaken free of charge, except where requests are unfounded or excessive.⁷⁵ Data subjects are afforded, among other rights, the right to (i) be notified about data collected from data subjects⁷⁶ or third parties,⁷⁷ and in such cases be provided with information to aid

62 GDPR art 5(1)(c).

63 GDPR art 5(1)(e).

64 GDPR art 5(1)(f).

65 GDPR art 6(1)(a).

66 GDPR art 6(1)(b).

67 GDPR art 6(1)(c).

68 GDPR art 6(1)(d).

69 GDPR art 6(1)(e).

70 GDPR art 6(1)(f).

71 *Guidelines* (n 18) 9.

72 *Art 29 Guidelines* (n 18) 5.

73 GDPR art 12(1).

74 GDPR arts 12(2), (3) & (4).

75 GDPR art 12(5).

76 GDPR art 13.

77 GDPR art 14.

transparency; (ii) access data;⁷⁸ (iii) rectify data;⁷⁹ (iv) erase data⁸⁰ ('the right to be forgotten'); (v) restrict the processing of data; and (vi) object to the processing of data.⁸¹

In respect of ADM and profiling, notification and access rights explicitly acknowledge these processes and require that data subjects either be notified⁸² of, or have access⁸³ to 'the existence of automated decision-making, including profiling ... and, at least in those cases, *meaningful information* about the *logic involved*, as well as the *significance* and the *envisaged consequences* of such processing for the data subject'.⁸⁴

While this 'explanatory provision' may appear promising, I ~~note four limitations~~. First, the obligation to notify data subjects about such processing in terms of article 13(1) is limited to 'the time when personal data are obtained'⁸⁵ and places no further obligation on a controller to inform a data subject *ex post*. At the time of notification, ADM or profiling may not have taken place, and in such cases it would be impossible to pre-emptively provide 'meaningful information' or 'envisaged consequences'. Also, data mining using ML algorithms is a 'highly dynamic process',⁸⁶ the logic of which evolves over time, thus making explanations very difficult, if not impossible.

Second, concerning information that is not obtained directly from data subjects (article 14), I emphasise that neither GDPR nor the WP29 guidelines⁸⁷ consider observations, inferences or knowledge discovered about a data subject through a data-mining process as an alternative source of personal data, and in turn, the notification requirements (towards data subjects) under article 14 do not apply. In a BD and AmI scenario, the most valuable information ('knowledge') relating to a data subject is not obtained directly from a data subject but rather through 'descriptive' and 'predictive' data mining.⁸⁸

78 GDPR art 15.

79 GDPR art 16.

80 GDPR art 17.

81 GDPR art 21.

82 GDPR arts 13-14.

83 GDPR art 15.

84 GDPR arts 13(2)(f), 14(2)(g) & 15(1)(h) (my emphasis).

85 GDPR art 13(1).

86 Kamarinou and others (n 26) 4.

87 *Guidelines* (n 18) para 23.

88 BW Schermer 'The limits of privacy in automated profiling and data mining' (2011) 27 *Computer Law and Security Review* 46.

Third, regarding the right of access to information, article 15(1) sets out that data subjects have the right to obtain confirmation as to whether or not their personal data is being processed, as well as a copy thereof.⁸⁹ When read with the above ‘explanatory provision’, it appears that article 15 is the closest embodiment of a ‘right to explanation’ under the GDPR, in that unlike articles 13 to 14, it may be invoked *ex post* ADM or profiling processes. However, it is imperative to point out that this right of access is subject to article 15(4) which requires that any access to information does not ‘adversely affect the rights and freedoms of others’.⁹⁰ In the context of a controller who utilises ADM or profiling as part of its business model, providing an explanation as to the ‘logic involved’ may be argued to impact on intellectual property or trade secrets of the controller. The fourth and final limitation relates to the semantics of the ‘explanatory provision’ and impacts on all of the aforementioned rights already described. That said, Wachter, Mittelstadt and Floridi argue that the semantics of the provision point to a right of explanation relating to ‘system functionality, not the rationale and circumstances of specific decisions’⁹¹ – the consequence being that there is no transparency about the reasons for specific decisions.

The second principle of ‘purpose limitation’ described by article 5(1)(b) not only requires that the collection of personal data be for ‘specified’, ‘explicit’ and ‘legitimate’ purposes, but that the further processing of personal data be principally limited to the initial purpose for which the data was initially collected.⁹² Savin succinctly describes this principle as ‘delegitimising secondary uses of data’.⁹³ This principle ought to be considered in light of the aforementioned ‘data minimisation’ and ‘storage limitation’ principles – which may be inherently difficult to reconcile for controllers engaged in ADM or profiling practices as ‘data minimisation is inimical to the underlying thrust of BD’.⁹⁴ In this light, the right to object to the processing of personal data in cases of profiling is expressly limited to instances where a controller is lawfully processing a data subject’s personal data on the grounds of either ‘public interest’⁹⁵ or ‘legitimate interests’.⁹⁶ In other words, where processing is based on consent or one of the other lawful grounds, a data subject cannot object but at most may withdraw

89 GDPR art 15(3).

90 GDPR art 15(4).

91 Wachter and others (n 35) 9.

92 GDPR art 5(1)(b).

93 Savin (n 29) 257.

94 Rubenstein (n 3) 78.

95 GDPR art 6(1)(e).

96 GDPR art 6(1)(f).

consent and cease utilising the controller's services – this imbalance of power is something to be monitored.

The third and last principle mentioned herein is that of accuracy. In the context of profiles (and decisions that are based on profiles), 'clean', accurate data is essential for data mining techniques – especially those 'predictive' in nature. Thus, where inaccurate profiles have been created, upon which inaccurate decisions have been made, it becomes vital that a data subject has the right to rectify,⁹⁷ erase⁹⁸ or restrict⁹⁹ such processing activities. Under GDPR, the right to rectification is unconditional, and the right to restriction of processing considers inaccuracy of data as a valid ground for restriction.¹⁰⁰ The right to erasure, however, does not contemplate profiling or inaccuracy as a ground for invocation of the right. Instead, it allows for erasure based on a successful objection by the data subject. Yet, as elucidated above, the right to object is narrowly drafted to only be applicable when processing is based on certain grounds and, therefore, this right does not serve as much utility as the right to rectify or restrict.

In concluding GDPR's first prong, it is noted that extra protections are provided to data subjects including the right to data portability.¹⁰¹ Furthermore, the unique requirements of privacy by design¹⁰² and data protection impact assessments where the 'systematic and extensive evaluation of personal aspects relating to natural persons'¹⁰³ takes place, are particularly reassuring – especially when viewed in conjunction with GDPR's requirement of 'prior consultation' (discussed more fully in part 4). Nevertheless, while being extensive, several aspects of GDPR's first prong have been shown to be limited in the context of ADM and profiling processes.

3.3.2 *POPIA prong one*

Whereas GDPR's first prong separates its processing principles, lawful grounds for processing and data subject rights (which receive a dedicated chapter), POPIA's first prong intertwines its lawful grounds for processing and data subject rights within its processing conditions. To aid comparison,

97 GDPR art 16.

98 GDPR art 17.

99 GDPR art 18.

100 GDPR art 18(1)(a).

101 GDPR art 20.

102 GDPR art 25.

103 GDPR art 35(3)(a).

I will therefore assess POPIA's first prong in a similar sequence to that of GDPR.

POPIA's eight conditions for lawful processing are listed in section 4 and all stem from the first principle of 'accountability'¹⁰⁴ which requires compliance with POPIA throughout the processing life cycle. In terms thereof, personal information must be collected for specified purposes¹⁰⁵ and processed in a limited,¹⁰⁶ open,¹⁰⁷ accessible,¹⁰⁸ (iv) accurate¹⁰⁹ and (vi) secure manner.¹¹⁰

Starting with the 'processing limitation' condition, processing will be lawful and justified if predicated on one or more of the following grounds: (i) consent;¹¹¹ (ii) contractual obligations;¹¹² (iii) legal obligations;¹¹³ (iv) legitimate interests of a data subject;¹¹⁴ (v) public law duties;¹¹⁵ and/or (vi) the legitimate interests of a responsible party or of a third party.¹¹⁶ Such processing must also be 'adequate, relevant and not excessive'¹¹⁷ in terms of the 'minimality condition' – which ultimately runs contrary to the nature of data mining processes. Lastly, a right to object is also provided for, subject to the same limitations as those in GDPR, with the addition of an alternative grounds of processing ('legitimate interests of the data subject').¹¹⁸

Closely connected, POPIA's 'further processing limitation' goes on to provide that any further processing must be compatible with the purpose for which it was collected¹¹⁹ and that when testing for compatibility, 'the

104 POPIA sec 8 (Condition 1).

105 POPIA secs 13-14 (Condition 3).

106 POPIA secs 9-12 (Condition 2) and POPIA sec 15 (Condition 4).

107 POPIA secs 17-18 (Condition 6).

108 POPIA secs 23-25 (Condition 8).

109 POPIA sec 16 (Condition 5).

110 POPIA secs 19-22 (Condition 7).

111 POPIA sec 11(1)(a).

112 POPIA sec 11(1)(b).

113 POPIA sec 11(1)(c).

114 POPIA sec 11(1)(d).

115 POPIA sec 11(1)(e).

116 POPIA sec 11(1)(f).

117 POPIA sec 10.

118 POPIA sec 11(1)(d).

119 POPIA sec 15(1).

consequences of the intended further processing for the data subject'¹²⁰ must be taken into account, thereby serving as a useful yardstick for responsible parties when undertaking ADM processes.

Under its 'openness' condition, POPIA, like GDPR, requires a transparent relationship between responsible parties and data subjects so as to ensure that data subjects can understand what their rights are, and when to invoke them. Interestingly the 'openness' condition also requires responsible parties to keep a record of all processing activities. However, where ADM or profiling involve de-identified information, this obligation would not be applicable due to limitations on the definition of 'personal information' already discussed. Moving on, under POPIA's first prong data subjects have the rights to (i) receive notification when personal information is collected from a data subject or a third party and what such processing entails;¹²¹ (ii) access information;¹²² (iii) correct and request the destruction or deletion of information;¹²³ and (iv) object¹²⁴ to the processing of personal information.

In respect of POPIA's notification, collection and access rights, I note the following. First, unlike GDPR's 'explanatory provision', a right of explanation regarding ADM or profiling processes is not provided for in POPIA's first prong. Instead, a right of explanation is considered within its second prong, which will be discussed below in part 3.3.4. Second, while at first glance POPIA's collection rights appear to go further than those within GDPR – by requiring that personal information be collected directly from data subjects¹²⁵ – POPIA nonetheless recedes. What I am pointing to here is POPIA's waiver provisions located within its aforesaid notification and collection rights. Thereunder, data subjects may consent to (i) the collection of personal information from another source and (ii) non-compliance by a responsible party with their notification duties prescribed in section 18.¹²⁶ In such cases there is the danger that data subjects may unknowingly waive their rights to the transparent collection and processing of their personal information, *ex post* the conclusion of a contract, privacy policy or other binding document regulating the responsible party-data subject relationship. Under this provision, the danger continues in that not only may responsible parties be allowed to

120 POPIA sec 15(2)(c).

121 POPIA sec 18.

122 POPIA sec 23.

123 POPIA sec 24.

124 POPIA secs 11(3) & 18(1)(h)(iv).

125 POPIA sec 12(1).

126 POPIA sec 18(4)(a).

indirectly source personally identifiable information, but when coupled together with a waiver of notification rights, responsible parties would legally be allowed to keep such collection and processing activities from a data subject, unless an access request is made. I therefore contend that these waiver provisions, with an emphasis on section 18(4)(a), may pose a risk to the liberties of data subjects, especially in the context of BD and AmI processes, and ought to be subject to constitutional scrutiny.

Insofar as POPIA's right of access is concerned, its use is severely limited. Apart from not providing for a right of explanation of ADM or profiling processes, a data subject may at best 'request from a responsible party the record or a description of the personal information about the data subject held by the responsible party'.¹²⁷ Moreover, in such cases a responsible party may raise a ground of refusal to such request in terms of the Promotion of Access to Information Act 2 of 2000.

Regarding the information quality (accuracy) condition, POPIA closely mirrors GDPR's rights to rectify,¹²⁸ erase¹²⁹ and restrict¹³⁰ processing. It also places an onus on responsible parties to ensure the accuracy of personal information by way of 'reasonably practicable steps'.¹³¹ In an ADM or profiling context, it is not clear what would constitute 'reasonable steps' owing to the unpredictable nature of data mining processes.

Lastly, in regard to the retention of records, POPIA requires responsible parties to not retain personal information 'longer than is necessary for achieving the purpose for which the information was collected or subsequently processed'.¹³² This safeguard nevertheless is subject to the exceptions following therefrom, allowing retention on the basis of consent, performance of contractual obligations or purposes reasonably required for the functioning or activities of a responsible party¹³³ – all of which may be raised by a responsible party engaged in ADM or profiling practices. It is interesting to highlight, however, that section 14(3) places an obligation on responsible parties to retain any personal information used in a decision-making process for a period of time as prescribed by a law, code of conduct or, where none exists, for a reasonable time that enables a data subject to request access to such record. I contend that on

127 POPIA sec 23(1)(a).

128 POPIA sec 24(1).

129 As above.

130 POPIA sec 14(6).

131 POPIA sec 16(1).

132 POPIA sec 14(1).

133 POPIA sec 14(1)(b).

the basis of this ‘accountability mechanism’, it is plausible that a data subject may request access to a profile that has not yet been de-identified, and which has been used in a decision-making process.

To conclude POPIA’s prong one rights, it is reiterated that while they follow GDPR’s prong one rights quite closely (and develop notable accountability mechanisms) there is a significant degree of room granted to responsible parties for non-compliance with their obligations on the basis of ‘consent’.

3.3.3 *GDPR prong two*

In respect of GDPR’s second prong, solely ADM, including profiling, is specifically addressed under GDPR article 22. In terms of article 22(1), data subjects are afforded the right ‘not to be subject to a *decision* based *solely* on automated processing, *including profiling*, which produces *legal effects* concerning him or her or similarly *significantly affects* him or her’.¹³⁴

At the outset of this analysis, it is imperative to note that the drafting of article 22(1) is notoriously ambiguous and has given rise to two significant interpretive questions, the answers to which ultimately shape the extent and adequacy of protection against unlawful ADM and profiling practices under GDPR. The first question relates to the nature of the right contained in article 22(1) and revolves around whether the right constitutes either an ‘election’ (data subjects may object to the processing and nullify the decision) or a ‘prohibition’ (an automatic ban is placed on article 22(1) decisions). The second question is whether, in the absence of decision making, profiling is regulated.

Beginning with the first question, the EPDB has taken the position that the right should be interpreted as a general prohibition on the basis that this interpretation is in alignment with the fundamental principles of GDPR and the fundamental human rights GDPR seeks to protect.¹³⁵ In taking this stance, it refers to Recital 71 which speaks of specific instances where the processing considered in article 22(1) ‘should’ be allowed – by inference, meaning that such processing, by default, is prohibited. The ‘prohibition’ interpretation has been assented to by Wachter and

134 GDPR art 22(1) (my emphasis).

135 *Guidelines* (n 18) 20.

others¹³⁶ as well as by Kaltheuner and Bietti.¹³⁷ Further, it was followed by ‘Austria, Belgium, Germany, Finland, the Netherlands, Portugal, Sweden and Ireland’¹³⁸ under the DPD’s similarly-constructed provision.¹³⁹ Meanwhile, others like Bygrave¹⁴⁰ and Savin¹⁴¹ have opined that the right should be interpreted as an election to object to such processing. The ‘election’ interpretation was also followed by the United Kingdom under the DPD. In December 2023 EU jurisprudence finally offered a binding interpretation of article 22(1), wherein the Advocate General of the Court of Justice of the European Union (CJEU), in the *Schufa* case, held that “[d]espite the terminology used, the application of Article 22(1) of the GDPR does not require the data subject to actively invoke the right”.¹⁴² The CJEU went on to affirm this interpretation and clarified that the right in article 22(1) is indeed a prohibition against solely ADM.¹⁴³

In approaching the second question, I will begin with Recital 71. Thereunder, the legislators suggest that automated processing – in terms of article 22(1) – ‘includes “profiling” that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person’.¹⁴⁴ The Recital goes further to state that the term ‘decision’ referred to in article 22(1) ‘may include a measure, evaluating personal aspects relating to him or her’.¹⁴⁵ Accordingly, Recital 71 considers a profile constructed by automated means as a decision in and of itself and, thus, suggests that article 22(1) caters for the creation of profiles. Conversely, Wachter and others, Mittelstadt and Floridi¹⁴⁶ as well as Kaltheuner and Bietti¹⁴⁷ have viewed article 22(1) as not considering profiling in the absence of decision making. Yet, notwithstanding academia’s opposing

136 Wachter and others (n 35) 20.

137 F Kaltheuner & E Bietti ‘Data is power: Towards additional guidance on automated-decision making and profiling in the GDPR’ (2017) 2 *Journal of Information Rights, Policy and Practice* 11.

138 Wachter and others (n 35) 19.

139 See DPD art 15.

140 L Bygrave ‘Automated profiling: Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling’ (2001) 17 *Computer Law and Security Review* 17-24.

141 Savin (n 29) 257.

142 Opinion of Advocate General in *OQ v Land Hessen and Schufa Holding AG (as intervener)* 16 March 2023.

143 *OQ v Land Hessen and Schufa Holding AG (as intervener)* (C-634/21) 7 December 2023 para 52.

144 GDPR Recital 71.

145 As above.

146 Wachter and others (n 35) 20.

147 Kaltheuner & Bietti (n 138) 11.

views Recital 71 is now corroborated by recent developments in the *Schufa* case, where the CJEU held that if a profile serves a ‘determining role’ in a decision, that profile will constitute a decision in and of itself, even where the Controller who generated the profile is not the decision-maker.¹⁴⁸

Building on the above, I postulate the following thoughts: First, if article 22(1) was intended to constitute an ‘election to object’, it is arguable that the drafters would have clearly incorporated ADM, including profiling, as an objectionable ground within the ‘right to object’ in article 21(1). Second, and from a different angle, one may argue that because ‘profiling’ is included as a ground of objection under article 21(1) – and ADM is not – the legislators intentionally separated the two processes, providing a right to object for profiling in article 21(1), and a prohibition for solely automated ADM (even if based on profiles) in article 22(1). Lastly, the ‘suitable measures’ (discussed below) that must be put in place to safeguard data subject rights and freedoms are only required when article 21(1) is not applicable. Accordingly, I contend that if article 21(1) was intended to constitute an ‘election’, then the drafters would have required the aforementioned ‘suitable measures’ to be put in place where a data subject fails to make an ‘election’. The absence thereof suggests that there is no need for suitable measures in the first place as the conduct to which the safeguards would apply is already prohibited.

Moving on, the applicability of the provision is constrained in two respects. First, protection is only operative when all of the definitional elements as contained therein are present, those being that (i) the data subject must have been subjected to a decision; (ii) the decision must have been reached solely by automated processing; and (iii) the decision must have produced legal effects and/or must pose a risk of significantly affecting the data subject.¹⁴⁹ It should be noted that although GDPR defines neither ‘legal effects’ nor ‘significant effect’, the EDPB has published guidelines to assist in the interpretation thereof.¹⁵⁰ Therein it regards ‘legal effects’ as decisions that affect one’s legal rights and has adopted a subjective approach to ‘significant effect’, which may place an onus on data subjects to prove significance.¹⁵¹ I wish to emphasise that in the context of AmI, it is possible that numerous seemingly ‘insignificant’ effects, can accumulate into a significant effect (in the form of subtle manipulation or ‘hacking’

148 *Scufa Holding* Case C-634/21, para 50. Judgment of the first chamber. <https://curia.europa.eu/juris/liste.jsf?num=C-634/21> (accessed 1 December 2023).

149 GDPR art 22(1).

150 *Guidelines* (n 18).

151 *Guidelines* (n 18) 21.

as envisaged by Harari)¹⁵² – a scenario that has not been acknowledged by the EDPB.

Second, article 22(1) only protects data subjects in the absence of article 22(2)(a)-(c) exceptions, namely, contractual obligations,¹⁵³ explicit consent¹⁵⁴ and authorisation under a '[European Union] or member state law to which the controller is subject'.¹⁵⁵ In the event that article 22(1) is not applicable, controllers ought to implement 'suitable measures' that may include providing data subjects with the rights to (i) obtain human intervention; (ii) express one's point of view; and (iii) contest the decision.¹⁵⁶ At this juncture I note that despite Recital 71 suggesting that safeguards 'should' include 'a right to explanation of the decision', this right has not been incorporated into article 22 as an operative provision and, consequently, data subjects will need to rely on article 15 – albeit being limited in application. Lastly, as far as special category personal data¹⁵⁷ is concerned in the aforesaid instance, such data may only be utilised if the data subject has given explicit consent¹⁵⁸ or the processing is 'necessary for reasons of substantial public interest'.¹⁵⁹

In concluding GDPR's prong two rights, it is submitted that they lack definition and require judicial clarification to determine their exact nature and scope.

3.3.4 POPIA prong two

In respect of the second prong, ADM is specifically addressed under section 71 of POPIA titled 'Automated decision making'. In terms of section 71(1), data subjects

may not be subject to a *decision* which results in *legal consequences* for him, her or it, or which *affects* him, her or it to a *substantial degree*, which is based *solely* on the basis of the automated processing of personal information *intended to provide a profile* of such person including his or her performance at work, or his,

152 Harari (n 1).

153 GDPR art 22(2)(a).

154 GDPR art 22(2)(b).

155 GDPR art 22(2)(c).

156 GDPR art 22(3).

157 GDPR art 9(1).

158 GDPR art 22(4) as read with art 9(2)(a).

159 GDPR art 22(4) as read with art 9(2)(g).

her or its credit worthiness, reliability, location, health, personal preferences or conduct.¹⁶⁰

Unlike the (now resolved) ambiguity surrounding the nature of GDPR's article 22(1), POPIA's prong two right is clearly prohibitive and need not require any further analysis. However, in as far as the scope of the right is concerned, there appears to be confusion among South African academia that stems from an inaccurate conceptualisation of the processes of ADM and profiling, resulting in misinterpretations of the law.

As was made clear in part 2, ADM and profiling are distinct processes that may overlap in practice – specifically when profiles are applied in the process of decision making. However, I also emphasised that profiles can serve other functions when re-applied in a data-mining process and are therefore not limited to being applied in the course of decision making. Saying that, Naude views the section 71(1) prohibition as 'relating to automated decision making (also known as profiling)'.¹⁶¹ Similarly, Roos holds that 'automated decision making is sometimes also called profiling'.¹⁶² I respectfully submit that the aforesaid academics have overlooked that these two processes are distinct.

A by-product of the above confusion is that section 71(1) is misinterpreted. In their book Burns and Burger-Smidt state that '[t]he South African legislature has been alert to the dangers of processing personal information for the purposes of profiling and has expressly prohibited processing for this purpose in section 71 of the POPI Act'.¹⁶³

On a similar note, the authors have affirmed their stance by arguing, with reference to section 71(1), that 'the POPI Act expressly prohibits the creation of a profile on the basis of automated processing'.¹⁶⁴ Again, and with respect, I contend that Burns and Burger-Smidt are mistaken. I argue instead that the right does not apply to profiling *per se*, but rather to decisions reached on the basis of solely automated profiling. By implication, I am also arguing that decisions that are reached in the absence of the solely automated application of a 'profile' fall outside the

160 POPIA sec 71(1) (my emphasis).

161 A Naude 'Data protection in South Africa: The impact of the Protection of Personal Information Act and recent international developments unpublished LLM dissertation, University of Pretoria, 2014 55.

162 A Roos 'Data privacy law' in D van der Merwe, A Roos & T Pistorius (eds) *Information and communications technology law* (2016) 462.

163 Burns & Burger-Smidt (n 38) 329.

164 Burns & Burger-Smidt (n 38) 331.

ambit of protection provided for in section 71(1). A final (non-technical and purely semantical) point I will raise is that the wording throughout POPIA (in the section title, as well as in section 60(4)(a)(ii) in respect of codes of conduct) both merely refer to ‘automated decision making’ – thereby pointing at the drafters’ intention to regulate ADM, and not profiling.

Having clarified the scope of section 71(1), I turn to the terms ‘legal consequences’ and ‘substantial degree’ that create a threshold within the right. These terms are not defined, and at the time of writing there are no regulations, opinions or guidelines published by the South African Information Regulator to assist in applying these thresholds. When providing guidance on these thresholds, I recommend that the Information Regulator considers the ‘cumulative effect’ of seemingly insignificant decisions (as described above).

In further limiting the right in section 71, section 71(2) provides exceptions in the case where the decision is (i) taken in light of the conclusion or execution of a contract, where a data subjects request in terms of a contract has been met;¹⁶⁵ or where (ii) ‘governed by a law or code of conduct’.¹⁶⁶ In both the aforesaid instances, section 71(3) requires responsible parties to put ‘appropriate measures’ in place for data subjects. These measures should provide data subjects with an opportunity to make informed representations about a solely automated decision¹⁶⁷ by providing data subjects with ‘sufficient information about the underlying logic of the automated processing of the information relating to him or her’.¹⁶⁸ Commendably, the foregoing measures constitute an undeniable right to explanation that has been shown to be absent under GDPR. Yet, critically, section 71 does not specify anything concerning instances where ‘special personal information’¹⁶⁹ or information on children is used to make automated decisions.

In concluding POPIA’s second prong, I reiterate that there is no scope for protection against unfair profiling practices and that decisions made in the absence of an applied profile have also been shown to be unregulated. POPIA’s right of explanation, however, must be praised.

165 POPIA sec 71(2)(a)(i).

166 POPIA sec 71(2)(b).

167 POPIA sec 71(3)(a).

168 POPIA sec 71(3)(b).

169 POPIA sec 1.

4 Contextualising current regulation in an age of big data and ambient intelligence

4.1 Findings on extent

4.1.1 *A deep-rooted lacuna*

In part 3.2 I highlighted that the foundational definitions of ‘personal data’ and ‘personal information’ under GDPR and POPIA, respectively, indicate that the extent of protection is limited to information that is personally identifiable. This limitation is expressly confirmed in both laws.¹⁷⁰ Despite an attempt in GDPR to provide protection for de-identified personal data that is capable of being re-identified, I have contended that the provision is conflicted and lacking in enforceability. POPIA, on the other hand, simply does not provide protection in such instances. Consequently, I find that none of the rights discussed in part 3.3 above apply to de-identified personal information or group data. I draw attention to this limitation as a deep-rooted *lacuna* inherent not only in GDPR and POPIA, but in all data protection laws stemming from principles of the OECD Guidelines.¹⁷¹

4.1.2 *Opacity of the transparency principle*

In part 3.3 I described the rationale behind the processing conditions of ‘transparency’ and ‘openness’ as seeking to advance the informational self-determination of data subjects by enabling the enforcement of their rights when the processing of their data is unlawful, unfair or inaccurate. Yet, as Hildebrandt puts it, ‘even if the law attributes such rights of transparency and the right to resist automated decision making, these rights remain paper dragons as long as we lack the means to become aware of being profiled’.¹⁷²

In conjunction with the *lacuna* described above, I have found two catalysts that increase opacity between data subjects and responsible parties, ultimately rendering ‘the exercise of data subject rights highly theoretical’.¹⁷³ On the one hand, the lack of recognition of data mining as an essential source for the collection of personal information is detrimental

170 In respect of GDPR, see Recital 26. In respect of POPIA, see sec 6(1)(b).

171 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as amended on 11 July 2013.

172 Hildebrandt (n 4) 248.

173 B-J Koops ‘The trouble with European data protection law’ (2014) 4 *International Data Privacy Law* 252.

to transparency. Without notification, it is difficult, if not impossible, for data subjects to holistically gauge what new information is being mined, whether it is being de-identified, how it is being processed and what the consequences of such processing may be. On the other hand, in practice, responsible parties communicate – half-heartedly so – with data subjects via privacy notices and terms of use that describe instances where, and how, personal information is collected and processed. Therein, data subjects often consent to ‘umbrella clauses’ that widely describe the purposes of processing – often in the spirit of ‘providing a service’ – leaving room for further processing that in many instances cannot be described at the time of collection because ‘[responsible parties] do not (and cannot) know in advance what they may discover’.¹⁷⁴ It is welcoming to note, however, that since the inception of GDPR, EU supervisory authorities have adopted a strong stance¹⁷⁵ towards opaque processing activities, having fined Google LLC a record sum of €50 million on the basis of ‘lack of transparency, inadequate information and lack of valid consent’.¹⁷⁶

4.2 Assessing inadequacy

Evidently, GDPR and POPIA both suffer the same ‘regulatory dilemma’¹⁷⁷ – their processing principles (while being broad) are idealistic in the face of ADM and profiling practices, today, and more so, in an era of AmI that will ‘create new vulnerabilities and aggravate existing ones’.¹⁷⁸ Briefly stated, important legal and ethical issues¹⁷⁹ that will arise in an age of BD and AmI are (i) algorithmic errors; (ii) discrimination in decision making; (iii) the allocation of group profiles to individual data subjects (de-individualisation); (iv) loss of individual autonomy; and (v) information asymmetries between responsible parties and data subjects.

With this in mind, Hildebrandt and Koops maintain that in an age of AmI most profiling will be indirect, upon aggregated information relating to large groups of data subjects.¹⁸⁰ In such a case, GDPR and

174 Rubenstein (n 3) 78.

175 See, eg, Core Review ‘Major GDPR Fine Tracker – An ongoing, always-up-to-date list of enforcement actions’, <https://www.coreview.com/blog/alpin-gdpr-fines-list/> (accessed 15 September 2020).

176 CNIL ‘The CNIL’s restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC’, <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> (accessed 22 August 2020).

177 As above.

178 Hildebrandt & Koops (n 9) 433.

179 Hildebrandt & Koops (n 9) 434. See also Kamarinou and others (n 27) 46.

180 Hildebrandt & Koops (n 9) 434.

POPIA, as they stand, cannot be relied upon to protect data subjects from responsible parties who collect and apply new ‘knowledge’ that is mined from de-identified information. Moreover, as I alluded to above, the prong two rights of GDPR and POPIA are narrowly constructed to cater for instances where tangible, ‘significant’ or ‘legal’ effects on data subjects are observed. In an era of Aml, the ongoing, unobservable manipulation of what seem to be conscious thoughts, decisions and perceptions of data subjects may cumulatively result in significant effects that are unnoticeable in real time. This is what Zarsky refers to as ‘the autonomy trap’.¹⁸¹

4.3 Forward-looking recommendations

It is undoubtable that GDPR and POPIA, in their current form, are inadequate insofar as ADM and profiling are concerned. Therefore, the following recommendations are made, each of which may be viewed in isolation, or in unison.

4.3.1 A shift from regulating ‘collection’ to ‘usage’

The unfettered collection and processing of data on the basis of consent is not going to change, nor is the reliance of our digital society on BD data mining processes, the accuracy of which is reliant upon unconstrained masses of data.¹⁸² On this basis, I am in agreement with Zarsky’s assertion that the issues inherent in data mining may therefore best be addressed at the ‘usage’ stage as opposed to the ‘collection stage’ of data.¹⁸³ By focusing regulative efforts on ‘how’ data is being used in an ADM and profiling context, *sui generis* laws (highlighted below) may be developed to mitigate the shortcomings of current data protection law.

4.3.2 *Sui generis* laws

While the free flow of information is imperative in society and the economy of the twenty-first century and beyond, there will, in certain instances (such as those contemplated by prong two rights) be a need for ‘constitutive laws’ that enforce behaviour, as opposed to ‘regulative laws’ that aim to induce behaviour. Such ‘future generation’ data-protection laws have been proposed by Hildebrandt and take the form of (i) ‘transparency

181 T Zarsky ‘“Mine your own business!” Making the case for the implications of the data mining of personal information in the forum of public opinion’ (2003) 5 *Yale Journal of Law and Technology* 17.

182 T Zarsky ‘Online privacy, tailoring, and persuasion’ in KJ Strandburg & D Stan Raicu (eds) *Privacy and technologies of identity: A cross disciplinary conversation* (2006) 209-224.

183 T Zarsky ‘Responding to the inevitable outcomes of profiling’ in S Gutwirth, Y Pouillet & P de Hert (eds) *Data protection in a profiled world* (2010) 61.

enhancing tools' (TET's),¹⁸⁴ especially in cases of group profiling; (ii) 'ambient law' – wherein legal norms are embedded into the technical architecture of systems¹⁸⁵ under a principle of 'transparency by design'; and (iii) laws specifically predicated on protecting data subjects against the unwanted application of profiles.

Additionally, I insist that policy makers and international data-ethics communities lobby for updated OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – last updated in 2013 – that may build upon Hildebrandt's propositions and provide 'a new generation of data protection rules, wherein the "identifiability" of the data subject is no longer a criterion'¹⁸⁶ and where principles are designed around ADM and profiling from the ground up. These updated Guidelines should be considered for interoperability with the OECD Principles on Artificial Intelligence,¹⁸⁷ which include principles relating to human intervention in artificial intelligence systems, as well as transparency around artificial intelligence systems, artificial intelligence-based outcomes, and decisions reached through the use of such systems.

4.3.3 *External interventions*

I posit two final recommendations involving data protection authorities in the EU, and the Information Regulator in South Africa ('supervisory authorities'). First, supervisory authorities ought to consider their statutory powers under 'prior consultation',¹⁸⁸ 'prior authorisation',¹⁸⁹ and 'codes of conduct'¹⁹⁰ provisions within GDPR and POPIA, respectively. When considering prior consultation/prior authorisation provisions, there may be scope for the enforcement of specific notification requirements in instances of potentially prejudicial profiling practices. In a South African context, section 57(2) of POPIA provides that the Regulator may, by law or regulation, require other types of information processing to be subject to prior authorisation 'if such processing carries a particular risk for the legitimate interests of the data subject'.¹⁹¹ Furthermore, section 60 of POPIA empowers the Information Regulator to issue codes of conduct

184 M Hildebrandt 'Dawn of a critical transparency right for the profiling era' in J Bus and others (eds) *Digital enlightenment yearbook* (2012) 52-54.

185 Hildebrandt & Koops (n 9) 429.

186 Gutwirth & De Hert (n 17) 289.

187 OECD Principles on Artificial Intelligence (2020).

188 GDPR art 36.

189 POPIA sec 57(2).

190 POPIA sec 60(1) as read with sec 60(3)(c).

191 POPIA sec 57(2).

in various circumstances, including for ‘any specified activity or class of activities’¹⁹² which may include ADM and/or profiling.

Second, to rebalance information asymmetries, I propose the design and implementation of public databases, predicated on a right of access to information, wherein ‘tools to access both data and profiles [relating to] data subjects’¹⁹³ are provided under the oversight of supervisory authorities and human rights watchdogs. Such a database could be populated with ‘reported processing activities’. Within such a database, data subjects would be able to peruse all reported processing activities of responsible parties (or their operators) that are subject to the jurisdictional powers of a relevant supervisory authority. In this case, supervisory authorities may require any responsible party, who (i) processes personal information; (ii) engages in profiling; (iii) makes decisions based on personal information; or (iv) intends on further processing de-identified data, to report such processes. Unlike a ‘right of explanation’, such a system ought to be designed as a TET to assist data subjects in understanding, at a glance, which responsible parties are conducting profiling and what those profiles relate to, thereby allowing data subjects to invoke their prong one rights.

5 Conclusion

From semantic limitations and interpretive ambiguities, to deep-rooted *lacunae* and opaque transparency principles, an exploration of GDPR and POPIA (as jurisdictional yardsticks for global data-protection law) indicates that the protection of human liberties against proliferated ADM and profiling practices is inadequate in an age of BD and AmI. Instead of stretching these laws in their current form, specific, specialised legal and transparency-enhancing tools are required to rebalance information asymmetries between those who can ‘see’, and those who are being ‘seen’. The protection of human self-determination has become, and will continue to be, increasingly prevalent. As Franklin D Roosevelt and many others have held, ‘great power involves great responsibility’.¹⁹⁴ It is on this premise that solely automated decision-makers ought to be regulated.

192 POPIA sec 60(3)(c).

193 Hildebrandt & Gutwirth (n 17) 257.

194 FD Roosevelt ‘Undelivered address prepared for Jefferson Day’ (1945), [http:// www.presidency.ucsb.edu/ws/?pid=16602](http://www.presidency.ucsb.edu/ws/?pid=16602) (accessed 20 September 2020).

References

- Baratta, R 'Complexity of EU law in the domestic implementing process' (2014) 2 *TTPL* 293
- Bibri, SE *The shaping of ambient intelligence and the internet of things* (Atlantis Press 2015)
- Burns, Y & Burger-Smidt, A *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018)
- Bygrave, L 'Automated profiling: Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 *Computer Law and Security Review* 17
- Gutwirth, S & De Hert, P 'Regulating profiling in a democratic constitutional state' in Hildebrandt, M & Gutwirth, S *Profiling the European citizen: Cross-disciplinary perspectives* (Springer 2008) 288
- Harari, YN *Homo Deus: A brief history of tomorrow* (Harper 2016)
- M Hildebrandt 'Defining profiling: A new type of knowledge' in M Hildebrandt & S Gutwirth *Profiling the European citizen: Cross-disciplinary perspectives* (2008)
- Hildebrandt, M & Gutwirth, S *Profiling the European citizen: Cross-disciplinary perspectives* (Springer 2008)
- Hildebrandt, M & Koops, B-J 'The challenges of ambient law and legal protection in the profiling era' (2010) 73 *Modern Law Review* 3
- Hildebrandt, M 'Dawn of a critical transparency right for the profiling era' in Bus, J and others (eds) *Digital Enlightenment Yearbook* (IOS Press 2012) 52
- Hildebrandt, M 'Profiling and AmI' in Rannenberg, K, Royer, D & Deuker, A (eds) *The future of identity in the information society: Challenges and opportunities* (Springer 2009) 286
- Hildebrandt, M 'Who is profiling who? Invisible invisibility' in Gutwirth, S and others (eds) *Reinventing data protection?* (Springer 2009) 239
- Kaltheuner, F & Bietti, E 'Data is power: Towards additional guidance on automated-decision making and profiling in the GDPR' (2017) 2 *Journal of Information Rights, Policy and Practice* 11
- Kamarinou, D, Millard, C & Singh, J 'Machine learning with personal data' in Leenes, R, Van Brakel, R & Gutwirth, S (eds) *Data protection and privacy: The age of intelligence machines* (Hart Publishing 2017) 97
- Klimas, T & Vaiciukaite, J 'The law of recitals in European community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61

- Koops, B-J 'The trouble with European data protection law' (2014) 4 *International Data Privacy Law* 252
- Mordini, E & Tzovaras, D (eds) *Second generation biometrics: The ethical, legal and social context* (Springer 2012)
- Naude, A 'Data protection in South Africa: The impact of the Protection of Personal Information Act and recent international developments' unpublished LLM dissertation, University of Pretoria, 2014
- Roos, A 'Data privacy law' in Van der Merwe D, Roos A & Pistorius, T (eds) *Information and communications technology law* (LexisNexis 2016) 462
- Rubenstein, IS 'Big data: The end of privacy or a new beginning?' (2013) 3 *International Data Privacy Law* 2
- Savin, A 'Profiling in the present and new EU data protection frameworks' in Nielsen, PA, Schmidt, PK & Dyppel Weber, K (eds) *Erhvervsretlige emne* (Djøf Forlag 2015) 253
- Schermer, BW 'The limits of privacy in automated profiling and data mining' (2011) 27 *Computer Law and Security Review* 46
- Wachter, S, Mittelstadt, B & Floridi, L 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) *International Data Privacy Law* 20
- Wright, D, Gutwirth, S & Friedewald, M (eds) *Safeguards in a world of ambient intelligence* (Springer 2008)
- Zarsky, T "'Mine your own business!'" Making the case for the implications of the data mining of personal information in the forum of public opinion' (2003) 5 *Yale Journal of Law and Technology* 17
- Zarsky, T 'Online privacy, tailoring, and persuasion' in Strandburg, KJ & Stan Raicu, D (eds) *Privacy and technologies of identity: A cross-disciplinary conversation* (Springer 2006) 209
- Zarsky, T 'Responding to the inevitable outcomes of profiling' in Gutwirth, S, Pouillet, Y & De Hert, P (eds) *Data protection in a profiled world* (Springer 2010) 61

12

INDEPENDENCE OF DATA PROTECTION AUTHORITIES IN AFRICA: TRENDS AND CHALLENGES

Lukman Adebisi Abdulrauf

Abstract

The significance of a dedicated institutional framework for monitoring and enforcing the right to data protection cannot be overemphasised. Among the catalogue of human rights, it is one of a few with such privilege. This is not surprising, but considering the complexity of data processing, this has increased the need for a specialist oversight body. Almost all international data privacy instruments (now) require countries to establish these agencies. They further require that these agencies, generally called data protection authorities (DPAs), be independent. The African Union Convention on Cybersecurity and Personal Data Protection, for example, not only requires member states to establish DPAs but must ensure that they are 'completely independent'. Despite the significance of 'independence' in data protection law, understanding what it entails and achieving it seems complex, especially for African states. Therefore, the objective of this chapter is to consider the journey so far in applying the concept of independence of DPAs in Africa. The interlinked questions that the chapter seeks to answer are: to what extent have international principles on independence been implemented in Africa, and what are the trends and challenges, so far, in the application of the concept of independence of DPAs?

1 Introduction

The importance of data protection authorities (DPAs) to the overall realisation of the data protection project cannot be overemphasised. This is the reason why almost all modern data protection instruments require the establishment of such bodies. These instruments also grant DPAs with far-reaching powers in the processing of personal information by both public and private entities. Because of the nature and sensitivity of these enormous tasks they must perform, DPAs are required to be completely independent. Independence, therefore, has become a very critical concept under data protection law.¹ Despite some initial doubts, the inextricable link between independence and the effectiveness of a DPA seems to have

1 FH Cate and others 'The intricacies of independence' (2012) 2 *International Data Privacy Law* 1.

been firmly established today.² Independence, therefore, is very important for the effectiveness of a DPA because the very nature of their functions sometimes requires them to stand up against the powers of private entities and the government.

Africa is witnessing a significant renaissance in privacy and data protection and, as aptly put by Greenleaf and Cottier, '[n]ow it is Africa that is leading [the] global expansion [in data privacy], with 12 countries since 2013 adopting new laws'.³ Over the past few years, many African countries, indeed, have enacted data protection laws and established DPAs.⁴ Some of these DPAs are now fully functional, sometimes making bold decisions.⁵ However, the peculiar nature of the continent, which includes the fragility of its democracies and the far-reaching powers governments wield, means that independent regulatory agencies will face peculiar operational challenges. This is especially true for DPAs designed to make far-reaching decisions against the interests of the powerful. Many factors in Africa exist to always undermine their independence. In determining the extent of independence, the first place to look to is the statutes establishing the DPAs, which are the data protection laws of a country. Since international standards are now tilting towards detailed provisions, one can safely assume that the more detailed a statutory provision on independence, the better for independence. This, however, is not to undermine the peculiarities of individual countries, which calls for a contextual application of the concept. As rightly mentioned by Cate and others, 'independence may also be viewed differently in different legal cultures'.⁶

The objective of this chapter is to examine the experiences so far on the independence of DPAs in Africa with a view to showing trends and challenges. Specifically, the chapter questions the extent to which international legal standards on independence have been adopted (and

2 G Greenleaf 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer Law and Security Review* 3.

3 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' (2020) *University of New South Wales Law Research Series* 3, <http://classic.austlii.edu.au/au/journals/UNSWLRS/2020/32.pdf> (accessed 1 September 2021).

4 Out of the 55 African countries, 36 have enacted data protection laws. See Data Protection Africa 'Mapping 55 African countries | 36 data protection laws | 3 draft laws' <https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf> (accessed 3 March 2024).

5 Greenleaf & Cottier (n 3)7. Fifteen Out of the 32 countries with data protection instruments are yet to establish/appoint DPAs.

6 Cate and others (n 1) 1.

implemented) in data privacy instruments and legislation in Africa. This study is timely for two reasons. First, there has been limited comparative study on the application of independence of DPAs over the years.⁷ Thus, it is important to carry out such study for Africa considering the pace of reforms in data privacy around the continent. Second, the study of the application of independence in countries other than established democracies may, according to Tarosova, bring new perspectives to the issue.⁸ Therefore, Africa is an interesting case study in view of the sweeping wave of democratisation and constitutional reforms on the continent.

For purposes of this study, the term 'DPAs' will generally be used to refer to those public (or corporate) bodies that are responsible for overseeing or enforcing data protection norms. Furthermore, while Francophone African countries have been active in respect of data protection, this study focuses mainly on Anglophone Africa.⁹

2 International influence on the conceptualisation of 'independence' of DPAs

The determination of the meaning of the concept of independence of a DPA in data protection law is crucial for its proper application/implementation. Ordinarily, the concept implies a state of 'not [being] subject to control by others' or 'not requiring or relying on something else'.¹⁰ However, in law, this concept arguably has a narrower connotation, for it is not realistic in a constitutional democracy to have that sort of absolute independence as anticipated by its literal meaning. Generally, applying the concept of independence in law anticipates that certain public institutions should be able to carry out their statutory functions free from political influence or interference. It is a concept that originated in the United States, and its purpose is to insulate public bodies from political

7 Greenleaf (n 2) 4. The most comprehensive so far are the works of Greenleaf. See Greenleaf (n 2) 3-13. Regarding the Asian-Pacific region, see also G Greenleaf 'Independence of data privacy authorities (Part II): Asian-Pacific experience' (2012) 23 *Computer Law and Security Review* 121-128.

8 E Tarosova 'Data protection authorities in Central and Eastern Europe: Setting the research agenda' in P Jonason and others *The right of access to information and the right to privacy: A democratic balancing act* (2017) 144.

9 This is because of the challenge of translation of laws from Francophone countries. Even where these laws have been translated, such translations are not so reliable considering that they are not the official copies.

10 See *Merriam-Webster dictionary* online, <https://www.merriam-webster.com/dictionary/independent> (accessed 1 September 2021).

interference of political parties.¹¹ With advances in applying the doctrine of separation of powers, the concept of independence has been associated with the operation of certain public bodies.

While the first attempt to understand the concept of independence was made by scholars, international instruments, no doubt, have shaped the current understanding and application of the concept.¹² The first set of international data privacy instruments, the Organisation for Economic Cooperation and Development (OECD) Guidelines on Protection of Privacy and Transborder Flows of Personal Data 1980 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) 1981, did not provide for an institutional framework for the enforcement of data privacy norms. Thus, there was no question of the need for their independence. Subsequent instruments of these two international organisations, however, provided for such bodies. For example, the OECD Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy (2007) established a Privacy Enforcement Authority (PEA) but did not mention the need for its independence.¹³ According to Greenleaf, the United Nations (UN) General Assembly Resolution on Personal Data (1990)¹⁴ was the first international text to not only provide for establishing an enforcement authority but also require such authority to be independent. According to the Resolution, such authority ‘shall offer guarantees of impartiality, independence *vis-à-vis* persons or agencies responsible for processing and establishing data, and technical competence’.¹⁵ Apart from the non-binding nature of the Resolution, which limited its influence, this provision does not give clear guidance on what the concept entails. Nevertheless, at least, it opened the gates to the recognition of what would eventually become one of the most significant characteristics of a DPA.

The subsequent entry into force of the European Union (EU) Directive in 1995 concretised the requirement of independence of DPAs. Article 28 not only required state parties to establish DPAs, but that such authorities shall act with ‘complete independence’ in carrying out their functions. According to Greenleaf, ‘[b]y stating that all these functions must be exercised with “complete independence”’ the Directive makes

11 O Lynskey ‘The “Europeanisation” of data protection law’ (2017) 19 *Cambridge Yearbook of European Legal Studies* 257.

12 See works such as that of D Flaherty *Protecting privacy in surveillance societies* (1987).

13 For a more elaborate narrative, see Greenleaf (n 2) 3-13.

14 Guidelines for the Regulation of Computerised Personal Data Files, adopted by General Assembly Resolution 45/95.

15 Point 8 of the Resolution.

quite a strong statement about what “independence” means’.¹⁶ The EU Directive, however, does not give details on the components of ‘complete independence’. What may be gleaned from a plain reading of the provision is only an emphasis on sufficient powers for a DPA to make bold decisions and the fact that such decisions may be appealed in court. The ability to make bold decisions arguably is only a manifestation of independence and not necessarily a factor for independence. The only other provision regarding independence is Recital 62, which really adds nothing new to article 28. To consolidate the provisions of the Directive, the Charter of Fundamental Rights of the European Union (2000) not only recognised the right to data protection as a *sui generis* right but also provided that the right shall be enforced by an ‘independent authority’.¹⁷ No further details were provided as to what this independence entails. In all, the EU Directive, with its globalising effect, subtly induced other jurisdictions, including those of African countries, to make provisions on independence, sometimes without understanding the implications of the concept.

Since the EU Directive, subsequent reforms of data protection frameworks, especially in Europe, have taken note of the importance of legal provisions on independence and attempted to put finer details to it. Two such reforms are worth noting. The first is the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 (Convention 108+),¹⁸ which provides for complete independence.¹⁹ Further, the Convention only referred to the fact that in performing their duties, the supervisory authorities ‘shall not seek or accept instruction’.²⁰ It is unclear where such potential instruction that could impact ‘independence’ would be coming from, but it is plausible that the Convention envisages instructions from the government. Other provisions that relate to independence are the obligation upon state parties to provide sufficient resources for supervisory authorities to exercise their powers and that the decisions of supervisory authorities may be subject to appeals through the courts.²¹ The second reform in data protection is the

16 Greenleaf (n 2) 6.

17 Charter of Fundamental Rights of the European Union 2012/C 326/02, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT> (accessed 1 September 2021).

18 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (accessed 1 September 2021).

19 Convention 108+ art 15(5).

20 As above.

21 Convention 108+ arts 15(6) & (9).

coming of the EU General Data Protection Regulation (GDPR),²² which Hoofnagle and others have rightly described as ‘the most consequential regulatory development in information policy in a generation’.²³ So far, it contains the most detailed provision on independence. Article 52 of GDPR specifically provides for ‘independence’. According to GDPR:²⁴

- (1) Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
- (2) The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
- (3) Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
- (4) Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
- (5) Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
- (6) Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

From the above provision, one may draw some preliminary conclusions as to what the critical components of an independent DPA are. These are the ability to exercise their powers and function independent of external interference; the ability to act without external instructions, rule against engaging in incompatible occupations during their term in office; adequate human, technical and financial resources and infrastructures; the ability to

22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (accessed 1 September 2021).

23 CJ Hoofnagle and others ‘The European Union general data protection regulation: What it is and what it means’ (2019) 28 *Information and Communications Technology Law* 66.

24 GDPR (n 22) art 53.

choose and control its staff; a separate budget but subject to a financial control mechanism of the overall state or national budget. Article 52 may have incorporated some of the key elements of independence, but arguably it is not exhaustive. There are other important elements that complement independence, but which are only provided in other provisions of GDPR. For example, certain qualifications/qualities go with members of the supervisory authority, such as their mode of appointment, tenure, qualification, and method of removal. Indeed, achieving independence is dependent on a combination of complex factors, key among which attach to the holder(s) of the office of the DPA. Without those stipulations protecting the sanctity of the holder of the office, there is no way of achieving independence in practice. It probably is in recognition of this fact that GDPR goes a step further than all other international instruments by making detailed provisions in this regard.

It must be stated that some of the requirements mentioned for the first time in GDPR are not entirely new. After a comprehensive review of international sources before GDPR (especially various resolutions of DPA networks), Greenleaf identified five attributes of independence that are most common and seven others that are less common.²⁵ These are:

- (1) the establishment by legislation rather than any executive order or delegate legislation (firm legal basis);
- (2) the ability to investigate and report free of direction or permission from any other political or government authority;
- (3) a fixed term of office (commissioners should be appointed on a full-time basis);
- (4) removal from office only for defined reasons (inability, neglect of duty or serious misconduct) with procedural safeguards;
- (5) powers and duties to report directly on issues to either the parliament and/or the public.

The seven less common attributes identified by Greenleaf are the following:

- (1) immunity against personal lawsuits relating to the performance of official duties;
- (2) appointment by the legislature rather than the executive;
- (3) resources of the DPA determined independently of the executive;
- (4) positive qualification requirements for members/commissioners;
- (5) prohibition on commissioners undertaking other concurrent positions;
- (6) prohibition of appointment of commissioners from specified backgrounds that could cause a conflict of interests;

25 Greenleaf (n 2) 11.

(7) DPA decisions being subject to a right of appeal (to court).

The above succinctly explains what independence involves. As shown, independence in data protection law entails much more than what is ordinarily conceived. In my view, the attributes of independence can be broadly categorised into four groups. These are the attributes that go with functions and powers; mode of appointment and tenure and qualification of the office holders; adequate resources; and accountability. The attributes that go with the functions and powers of the DPAs include a stipulation that the DPA must be established by legislation;²⁶ freedom to exercise their powers without interference;²⁷ and immunity from lawsuits. The second category is that which relates to the mode of appointment and tenure. These include the provisions on the mode of appointment;²⁸ terms of office;²⁹ mode of removal;³⁰ and qualification.³¹ In the third category are those attributes regarding sufficient resources. In this regard, there are specifications that protect DPAs from any form of control in terms of resources (financial or personnel), which invariably means that they need to have sufficient resources.³² Finally, accountability provisions enable the powers of DPAs to be kept in check. They include provisions subjecting their finances to budgetary control,³³ and the right of appeal to courts against their decisions.³⁴ Accountability and transparency provisions are particularly useful, although they appear to add nothing substantial to an understanding the concept. According to Kuner and others,

the principle of independence is more complex than it may seem at first glance. While independence is indeed an indispensable requirement for the work of DPAs, complete and total independence is never possible, or even desirable, on the part of any public authority. Principles of accountability and transparency require that a supervisory authority be answerable for its

26 GDPR arts 54(1) & 51(1).

27 GDPR art 52(1).

28 GDPR art 53(1).

29 See generally GDPR art 54(1).

30 GDPR arts 53(3) & (4).

31 GDPR art 53(3); see also art 52(3) which speaks of members not engaging in an action that is incompatible with their duties or engage in any incompatible occupation. This, arguably, constitutes 'serious misconduct' and could be a ground for dismissal under art 53(3).

32 GDPR arts 52(4) & 52(5).

33 GDPR art 52(6).

34 GDPR art 58(4).

actions (eg, through the possibility of judicial review), and that it be subject to controls in order to ensure its integrity.³⁵

Considering that GDPR has incorporated most of these attributes in the four groups, one would expect that this will be the next international standard against which independence in data protection regimes of countries will be assessed. Indeed, the potential global reach of GDPR is not to be taken for granted, especially in Africa.³⁶ The next important question arises as to how the concept of independence of DPAs, so far, has been understood and applied in Africa.

3 Independence of DPAs in Africa

The application of the concept of independence is not new to Africa. Over time, certain statutory bodies have been established in some countries whose sole purpose is to promote democracy, and it is usually the requirement of the law that they should function independently. For example, in South Africa, these bodies, generally called ‘institutions supporting democracy’, are constitutionally established and bestowed with powers to promote transparency and accountability in governance.³⁷ The establishment of such bodies with the requirement of independence also finds support at the regional level with the African Charter on Democracy, Elections and Governance (African Democracy Charter), which requires state parties ‘to establish public institutions that promote and support democracy and constitutional order’.³⁸ Importantly, there is an obligation on state parties to constitutionally guarantee the independence and autonomy of these institutions.³⁹ Can DPAs be considered part of such institutions that aim to support democracy?

35 Cate (n 1) 1.

36 AB Makulilo ‘The GDPR implications for data protection and privacy protection in Africa’ (2017) 1 *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 12-19.

37 The Constitution of the Republic of South Africa, 1996 ch 9.

38 African Charter on Democracy, Elections and Governance art 15, <https://au.int/sites/default/files/treaties/36384-treaty-african-charter-on-democracy-and-governance.pdf> (accessed 1 September 2021).

39 African Democracy Charter art 15(2).

In this part, the approach towards the independence of DPAs at the regional-wide level will be considered before a review of the approach in selected African countries.

3.1 Regional context on independence of DPAs

Although regional data protection instruments, so far, have not had a significant influence on DPA regimes in Africa,⁴⁰ it is important to consider how the concept of independence is treated at the continental and regional levels. The foremost regional instrument on data protection, the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), provides in article 11 that each state party ‘shall establish an authority in charge of protecting personal data’ and such authority shall be ‘an independent administrative authority’.⁴¹ To further buttress the need for independence, the Convention provides that a member of the authority should not be member of the government or a business executive who owns shares in businesses in the ICT sector.⁴² This is as far the Malabo Convention goes in providing for independence. The Personal Data Protection Guidelines 2018 (Guidelines)⁴³ made pursuant to this Convention also do not add much flesh to the concept. While it recognises independence as a vital element for building trust online, it merely provides that a DPA is not likely to succeed in data protection ‘if it can be subjected to undue political, administrative or commercial pressure’.⁴⁴ The Guidelines mention some examples of factors that can affect independence, including where the staff of a DPA ‘are subject to undue political, administrative or commercial pressure’; where it is starved of sufficient enforcement powers and resources or subject to commercial lobbying or vexatious litigation.⁴⁵ While these are mere examples, they provide an insight into what the Guidelines consider important to gain independence.

Yet another continental-wide instrument that provides for independence is the Declaration of Principles on Freedom of Expression and Access to Information, which was prepared pursuant to article 45(1)

40 See AB Makulilo ‘The context of data privacy in Africa’ in AB Makulilo (ed) *African data privacy laws* (2016) 19.

41 Malabo Convention art 11(1).

42 Malabo Convention art 11(6).

43 Personal Data Protection Guidelines for Africa (Guidelines) 9 May 2018 21, https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 1 September 2021).

44 Guidelines (n 43) 16.

45 As above.

of the African Charter on Human and Peoples' Rights (African Charter) and adopted by the African Commission on Human and Peoples' in 2019.⁴⁶ In its provision on data protection, the Declaration urges states to establish independent entities for the protection of communications and personal information.⁴⁷ Furthermore, it provides that such entities should include human rights and privacy experts.⁴⁸ The general limitation of this instrument is that it actually seeks to foster the right to freedom of expression, and data protection is only incidental to it. Therefore, it may be presumed that where the right to freedom of expression and data privacy come in conflict, freedom of expression will prevail.

Unlike the Malabo Convention, the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection, one of the binding regional instruments on the continent, makes a more detailed provision on independence.⁴⁹ In providing that member states shall establish their own DPAs, the Supplementary Act stipulates that they shall be an 'independent administrative authority'.⁵⁰ It further provides for qualifications of the members, which shall be in law, information communication technology and any other relevant field.⁵¹ Members, according to the Supplementary Act, shall be incompatible with membership of government, exercise of business executives and ownership of shares in business in the information technology (IT) sector.⁵² It is also provided that members shall enjoy full immunity; however, the immunity is limited to 'opinions expressed in the exercise of, or during the tenure of their function'.⁵³

The next important regional instrument is the Southern African Development Community (SADC) Model Law on Data Protection.⁵⁴ It provides for the establishment of an independent and administrative

46 African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa, <https://www.achpr.org/legalinstruments/detail?id=69> (accessed 1 September 2021).

47 Declaration of Principles (n 46) Principle 42(8).

48 As above.

49 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, <https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf> (accessed 1 September 2021).

50 Supplementary Act (n 49) art 14(2).

51 Supplementary Act (n 49) art 15.

52 Supplementary Act (n 49) art 16.

53 Supplementary Act (n 49) art 17.

54 Southern African Development Community (SADC) Model Law on Data Protection, https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf (accessed 1 September 2021).

authority which ‘implies a decision-making power independent of any direct or indirect external influence on the Authority’.⁵⁵ Similarly, ‘the members shall remain independent from the influence of instruction of any other public authority’.⁵⁶ The Model Law provides for the competences of the permanent members. They must be competent in ‘personal data protection, privacy or communication and information technologies’.⁵⁷ Arguably, this is a more focused provision regarding competence acknowledging the fact that specific expertise is needed to run such an office. Furthermore, the SADC Model Law provides for the term of office⁵⁸ and the mode of removal of members of the DPA.⁵⁹ Finally, members of the DPA are granted immunity from views expressed in the execution of their duties.⁶⁰

African regional instruments contain rather instructive provisions regarding independence, even though still incomparable to the detailed provisions of GDPR. For example, all these instruments fall short in making provisions on the mode of appointment and the need for adequate resources of DPAs. In view of the centrality of these elements to the realisation of independence, their omission indeed is a clear flaw at the regional level. In conclusion, most of the regional instruments are independent initiatives with little or no connection to one another. They have, so far, had minimum impact at the domestic level.

3.2 Overview of the legal framework on ‘independence’ in selected countries

As mentioned, Africa is gradually becoming home to one of the fastest-growing data privacy regimes in the world. Based on the latest comprehensive study on Africa, there so far are 36 countries with data privacy legal frameworks in place.⁶¹ However, only about 16 of these have some sort of institutional framework for the enforcement of data privacy law. In this part I analyse the laws establishing some of the DPAs to show the nature and scope of the provisions on independence. To carry out this analysis, the approach of African countries in terms of statutory design can be broadly categorised into three (or four): the minimalist, moderate and robust. A fourth category is the extreme. Accordingly, regimes in the

55 SADC Model Law (n 54) sec 3.

56 SADC Model Law (n 54) sec 3(11).

57 SADC Model Law (n 54) sec 3(4).

58 SADC Model Law (n 54) sec 3(8).

59 SADC Model Law (n 54) sec 3(9).

60 SADC Model Law (n 54) sec 3(10).

61 Data Protection Africa (n 4).

robust category are countries with data privacy frameworks that provide for most of the international data privacy standards on independence contained in GDPR. The minimalist countries merely provide for independence without no elaboration of its basic attribute. The moderate falls in between both. At the extreme end are countries that do not even provide for independence at all or do not have a separate supervisory body for data protection.

South Africa arguably has the most elaborate incorporation of the international principles on independence in its Protection of Personal Information Act 2013 (POPIA).⁶² Although POPIA was largely tailored along the lines of the EU Directive, it contains many modern principles of GDPR.⁶³ The Act establishes the Information Regulator (IR) to supervise data privacy and access to information.⁶⁴ POPIA was explicit where it provides that the IR shall be 'independent and is subject only to the Constitution and to the law'.⁶⁵ This indeed is one of the most instructive stipulations on the legal basis. POPIA also provides that the IR must 'be impartial and perform its functions and exercise its powers without fear, favour and prejudice'.⁶⁶ In terms of POPIA, the IR can receive and investigate complaints free from any sort of external influence.⁶⁷ Similarly, the Regulators are appointed by the President on the recommendation of the National Assembly. They are also appointed for a fixed term of not more than five years and may be eligible for reappointment.⁶⁸ According to POPIA, they 'must be appropriately qualified, fit and proper persons'.⁶⁹ POPIA provides clearly defined reasons for removal from office, which include misconduct, incapacity and incompetence.⁷⁰ It also stipulates the procedure for the removal, which must be based on a finding by a committee of the National Assembly and supported by a

62 Protection of Personal Information Act 4 of 2013 (POPIA), https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf (accessed 1 September 2021).

63 For more in-depth analysis of this, see A Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected content principles' (2020) 53 *Comparative and International Law Journal of Southern Africa* 1-37.

64 POPIA, long title of the Act and sec 39.

65 POPIA sec 39(b).

66 POPIA sec 39(c).

67 POPIA sec 40(1)(d).

68 POPIA sec 41(2)(a).

69 POPIA sec 40(1)(b).

70 POPIA, sec 41(6).

resolution.⁷¹ To further buttress its independence, it is explicitly provided that the IR is accountable to the National Assembly⁷² and it can report directly to Parliament and the public.⁷³ Other provisions to guarantee its independence are the provision on immunity against personal lawsuits while performing its official duties; funds and resources of the Regulator being determined by Parliament independent of the executive;⁷⁴ and the prohibition on the appointment of regulators from certain backgrounds that could bring about a conflict of interest.⁷⁵

While the South African POPIA arguably provides for most of the international principles on independence, there are certain provisions that could impact independence. For example, the Regulator appointed full-time cannot perform any other remunerative work during the period he/she holds office except with the prior written consent of the Minister.⁷⁶ This provision subjects the Regulator to the executive as the Minister, in this case, is the cabinet member responsible for the administration of justice, who is a core member of the executive. Another curious provision that could impact independence is the requirement that the Regulator must consult the Minister of Finance in the exercise of its powers of appointment of staff.⁷⁷ While this may be justified on grounds of budgetary and financial planning purposes, it could be a conduit for more executive control of the IR. Nevertheless, this provision is in accordance with GDPR, which anticipates that the DPAs must be subject to relevant budgetary control from the appropriate government ministry.⁷⁸ However, perhaps this should be done in such a way as not to affect its independence.

Kenya belongs to the moderate category in the treatment of independence in the Data Protection Act 2019. It provides that the Data Commissioner shall act independently in the exercise of its powers.⁷⁹ The Act contains at least many of the key components of GDPR. The office of the Data Commissioner is established by statute as a state office in accordance with the Kenyan Constitution.⁸⁰ It can receive and investigate

71 As above.

72 POPIA sec 39(d).

73 As above.

74 POPIA sec 52.

75 POPIA secs 41(1)(g) & 45.

76 POPIA sec 41(1)(e).

77 POPIA sec 47(5).

78 GDPR art 52(6).

79 Kenya Data Protection Act 24 2019 sec 8(3).

80 In accordance with sec 260(q) of the Constitution of Kenya 2010. See Kenya Data Protection Act sec 5.

complaints.⁸¹ The Commissioner is appointed by the President with the approval of the National Assembly⁸² for a fixed term of six years⁸³ and can only be removed from office on clearly defined grounds.⁸⁴ The challenge with respect to the grounds of removal is a lack of clarity with regard to terms such as ‘incompetence’ or gross misconduct. This, indeed, is a general challenge with even GDPR, and all will depend on a careful interpretation by the courts. The Commissioner enjoys immunity from personal lawsuits.⁸⁵ The major challenge to independence of the Commissioner is the fact of the prominent role the Public Service Commission plays in its administration, which ordinarily is a key executive body. In terms of the Act, the Public Service Commission plays a key role in the appointment of the Commissioner⁸⁶ and other member of staff of the Officer.⁸⁷

Ghana’s approach falls within the minimalist category regarding the substance and details on independence. The Ghanaian Data Protection Act 2012 is centred around the Data Protection Commission. It has the power to investigate any complaint in a manner it considers fair, anticipating some sort of independence.⁸⁸ Unlike the South African and Kenyan approaches, the Ghanaian regime has many provisions that question the requirement of independence. The Board is the primary policy-making arm of the Commission, and it comprises members who are part of the executive branch, such as representatives from the National Communications Authority and Ministry of Communications.⁸⁹ The President appoints the members of the Board without any form of consultation.⁹⁰ The same goes for the appointment of the Executive Director who is appointed solely by the President.⁹¹ The Executive Director shall hold office ‘on terms and conditions specified in the letter of appointment’.⁹² More disturbing is the explicit provision on the ministerial directive which is to the effect that the Minister may give directives to the Board on matters of policy.⁹³ The

81 Kenya Data Protection Act sec 8(f).

82 Kenya Data Protection Act sec 6(3).

83 Kenya Data Protection Act sec 7(2).

84 Kenya Data Protection Act sec 11(d).

85 Kenya Data Protection Act sec 17.

86 Kenya Data Protection Act sec 6.

87 Kenya Data Protection Act sec 13.

88 Ghanaian Data Protection Act sec 3(c).

89 Ghanaian Data Protection Act sec 4(1).

90 Ghanaian Data Protection Act sec 4(2).

91 Ghanaian Data Protection Act sec 11(1).

92 Ghanaian Data Protection Act sec 11(2).

93 Ghanaian Data Protection Act sec 10.

executive also seems to be in control of the funds of the Commission in terms of the Act as sources of funds *inter alia* include ‘money approved by the Minister responsible for Finance’.⁹⁴ Perhaps it is no coincidence that that law never made any specific mention ‘independence’ of the Commission.

The Mauritius DPA is another regime that falls in the minimalist category. However, unlike the Ghanaian Data Protection Act, there is a clear stipulation on independence without the necessary details in its Data Protection Act 2017. The Act provides that ‘[t]he Office shall act with complete independence and impartiality and shall not be subject to the control or direction of any other person or authority’.⁹⁵ It also provides for the right of appeal to a tribunal from the decision of the Commissioner.⁹⁶ This is all it provides regarding independence, which is rather surprising considering that the Act is one of the most recent data protection laws on the continent. Makulilo was unequivocal with regard to the Mauritius Data Protection Act when he observed that

[o]ne shortcoming of the Data Protection Act is that, it does not clearly state to whom the Data Protection Commissioner is accountable to. He is only required to lay an annual report of the activities of the DPO before the National Assembly. Arguably, this leaves a lot to be desired in terms of the security of tenure of the Commissioner and may compromise the principle of independence. The same is true with regard to the financial independence of the DPO. The Act does not state where the budget of the Office comes from and how its availability is guaranteed without putting the independence of this Office under the mercy of administrative authorities.⁹⁷

Tunisia is also an interesting case where the Organic Act 2004-63 on the protection of personal data only recognises financial independence of the *Instance Nationale de Protection des Données Caractéristiques Personnelles* but still went on to provide that ‘the budget of the office is attached to the Ministry of Human Rights’.⁹⁸ It also scantily prohibits the President and members of the *Instance* from holding any interest in organisations relating to personal data processing.⁹⁹

94 Ghanaian Data Protection Act sec 14.

95 Mauritius Data Protection Act sec 4(2).

96 Mauritius Data Protection Act sec 51.

97 AB Makulilo ‘The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius’ (2021) 25 *International Journal of Human Rights* 133-134.

98 Organic Act 2004-63 of 27 July 2004 on the Protection of Personal Data art 75.

99 Organic Act (n 98) art 78.

Uganda is an example of a country at the extreme end of the continuum. Its Data Protection and Privacy Act 2019, made no provision for independence. This is not surprising considering the controversial type of democratic regime that holds sway in the country. The only semblance of provision for independence is the requirement that on the personal character of the director, who shall be a ‘person of high moral character, proven integrity and with relevant qualifications and experience’.¹⁰⁰ This stipulation, again, arguably is too vague. The Uganda Data Protection and Privacy Act also leaves a lot regarding the appointment of the National Data Protection Director, who is the head of the Personal Data Protection Office, to be determined by his/her instrument of appointment.¹⁰¹ Indeed, such an ‘instrument of appointment’ can contain all sorts of conditions that will undoubtedly affect independence. Still in the category of recent laws that do not give credence to the requirement of independence is the Zimbabwean Data Protection Act, which never made any provisions regarding independence.¹⁰² More surprising is the fact that it mandates data controllers to appoint data protection officers ‘charged with ensuring, in an *independent manner*, compliance with the obligations’ contained in the Act.¹⁰³ It is, therefore, strange that the Act requires independence for data protection officers of data controllers but not for the DPA.

From the above, it is clear that African countries need to do much more with regard to designing and implementing provisions on independence of DPAs. South Africa is one of the few countries with carefully-considered provisions, and it is hoped that this provision is sincerely implemented in practice.

4 Trends and challenges towards ‘independence’ of DPAs in Africa

The independence of a DPA, no doubt, is critical for the effective protection of the right to data privacy.¹⁰⁴ Data protection law, therefore, takes this requirement very seriously. The above analysis of the approach of African countries reveals that many countries have not paid close attention to the

100 Uganda Data Protection and Privacy Act 2019 sec 4(1).

101 See, e.g., Uganda Data Protection and Privacy Act 2019 secs 4(2) & (4).

102 Data Protection Act, No 5 2021, Available https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf (accessed 1 September 2021).

103 My emphasis. See sec 1, Zimbabwe Data Protection Act, 2021.

104 See T Davis ‘Data protection in Africa: A look at OGP member progress’ <https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf> (accessed 1 September 2021) 50.

technicality involved in the couching provisions on independence and its overall implication for independence in practice. In this regard, it is arguable that just the South African law makes a noteworthy provision on independence in terms of comprehensiveness. The point, however, must be re-emphasised that mere comprehensiveness of the provisions does not automatically translate into independence in practice. However, it is a first and, indeed, critical step towards attaining independence in practice especially for African countries. This part will now analyse some of the trends and challenges toward attaining the independence of DPAs in Africa. Since the experience of data protection on the continent is relatively nascent, the part will sometimes draw lessons from the experiences of other statutory bodies that are established to be independent in Africa.

Although the spread of data protection in Africa is rapid, there a general lack of appreciation of its intricacies.¹⁰⁵ The level of awareness of what is involved remains low and this could have a spiral effect on the extent of implementation.¹⁰⁶ Data protection is a technical aspect of law, and some level of expertise is needed to interact with this law. So far, while many African countries have adopted data protection legislations, many of these do so for purposes other than the realisation of human rights. For example, scholars have acknowledged the fact that the level of influence and the globalising effect of the EU regime is what has invariably forced many countries, especially in Africa, to adopt data protection laws.¹⁰⁷ If African countries do not appreciate the value of this subject, it will be difficult for them to sincerely establish supervisory agencies and grant them independent powers to function effectively. To justify this, it is easily noticeable on the continent that while many African countries have enacted data protection legislations, very few have established independent supervisory authorities and even fewer have these authorities already fully operational.¹⁰⁸

105 See generally LA Abdulrauf 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms' (2021) 30 *Information and Communications Technology Law* 87-107.

106 See generally LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

107 Makulilo (n 40) 19.

108 T Ilorin 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solution' 1, https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf (accessed 1 September 2021).

Apart from the lack of a sufficient understanding of the intricacies of privacy, which is manifested by the lack of political will to faithfully implement data protection standards, there also is the challenge of a shortfall in expertise to draft data protection laws. As earlier mentioned, data protection law is complex and there is a need for expertise. This expertise involved is not limited to a quality understanding of what the law involves, but also the ability to be able to track and transpose international development and standards in the law. In drafting the South African POPIA, the expert committee made an effort to track international development and ensure that this was reflected in the law. For example, the expert group carefully monitored the processes and discussions on GDPR even before it became fully operational.¹⁰⁹ Sufficient time was taken to develop a law that would stand the test of time. This is why the South African POPIA remains one of the continent's most detailed and carefully considered data protection instruments. Of course, this fact is vindicated by the nature and scope of the provisions on the independence of the Information Regulator considered above. The data protection laws of many other African countries contain very scanty provisions. This is even true for laws that were enacted after the entry into force of GDPR, such as the data protection law of Uganda. The Zimbabwe Data Protection Act is another example. In the Act, the powers of the Data Protection Authority are to be exercised by the Postal and Telecommunications Regulatory Authority.¹¹⁰ It is difficult to speak of independence with this kind of arrangement, and such an approach speaks to the lack of a sufficient understanding of the intricacies of data protection.

A manifestation of the lack of expertise that may impact provisions establishing DPAs in Africa is the trend towards appointing the heads or members of the supervisory authority just from any legal background and sometimes from the civil/public service without necessarily having expertise in data protection. As was mentioned in the previous part, the qualifications of members of the supervisory authority form part of independence. GDPR requires that 'each member shall have the qualifications, experience and skills, *in particular in the area of the protection of personal data*'.¹¹¹ In South Africa, the requirement of POPIA is that members of the Information Regulator 'must be appropriately qualified, fit and proper persons', which is understood, among others, as being experienced as a practising advocate or attorney or a professor of law at

109 See P Stein 'South Africa's EU-style Data Protection Law' (November 2012) *Without Prejudice* 48, <https://journals.co.za/doi/pdf/10.10520/EJC128763> (accessed 1 September 2021).

110 Zimbabwe Data Protection Act, 2021.

111 GDPR art 53(2) (emphasis added).

a university.¹¹² Similarly, the Mauritius Data Protection Act provides that to qualify as a commissioner, the person must be a lawyer with at least five years' standing at the bar.¹¹³ It is submitted that these backgrounds (or even a background in law specifically) do not necessarily make them experienced in data protection, which, as was earlier noted, is a technical field requiring specific expertise. The approach of the Kenyan DPA seems to be preferable because it provides that the Data Commissioner should hold a university degree in data science, law, information technology or any other related field.¹¹⁴ Although a law degree is required, it mentions other specialisations showing the technical and specialist experience. Though this may sound slightly ambitious, it is important that members of the DPA at least have some experience in data protection in addition to a legal background.

Obviously, the way in which provisions establishing DPAs are drafted goes a long way towards providing a platform for independence. A mere superficial provision does no good to the realisation of independence and could be a significant obstacle to achieving independence. In my view, this shows the extent of seriousness toward data protection on the continent. It must again be emphasised that the implementation and enforcement of these laws are another issue. Therefore, no matter how detailed a provision is on independence, the absence of political will to ensure its faithful implementation will always constitute a formidable challenge. Here, the disconnection between *de facto* and *de jure* independence is evident. Commentators have argued that legislations sometimes establish DPAs and claim they are independent, but such independence is only on paper.¹¹⁵ Indeed, Africa is seen as a region with rules and no real policing.

Yet another factor which may be a challenge to realising independence of DPAs in Africa is the general distrust by the African political class towards independent regulatory authorities. Though not supported by firm empirical evidence, these politicians make every effort to frustrate such bodies as shown in the experience with similar bodies like electoral commissions and anti-corruption agencies.¹¹⁶ This is especially true for countries with questionable democratic credentials, as even the judiciaries

112 POPIA sec 41.

113 Mauritius Data Protection Act sec 4(4).

114 Kenya Data Protection Act sec 7.

115 Davis (n 104) 50.

116 See generally CM Fombad 'The role of hybrid institutions of accountability in the separation of power scheme in Africa' in CM Fombad (ed) *Separation of powers in African constitutionalism* (2016) 325-344.

in such countries struggle to maintain their independence. This view was expressed Kuda Hove in a recent study that:

[t]here's this general distrust in having independent institutions in Africa. There is that distrust in having independent institutions in Africa. There is that distrust [that] if we grant them true autonomy, if we give them independence, they might turn against us in the future, that's sort of the feeling that governments have. So, to manage that fear, governments will then undermine their independence.¹¹⁷

A manifestation of this distrust is that while some countries have established DPAs, they still ensure that they are made an integral part of a government ministry. The Ghana Data Protection Commission is one of many examples. With such an arrangement, there is no way that the DPA can achieve independence. Another infamous example is that of Uganda. The Data Protection and Privacy Act clearly provides that the personal data protection office shall be 'under the Authority which shall directly report to the Board'.¹¹⁸ The Authority in this case is the National Information Technology Authority which is a key executive body. This used to be the case in Nigeria until 2023, when the Data Protection Act was enacted. The Nigerian Data Protection Regulation (NDPR), which was made by the National Information Technology Development Agency (NITDA) was implemented by NITDA (and subsequently the Nigeria Data Protection Bureau) which is one of the key agencies of government established under the Ministry of Communications and Digital Economy.¹¹⁹ The idea that data protection is just a mechanism toward advancing technology in a country and, therefore, subsuming the mandate of the supervisory agency under a government ministry is no good for the realisation of independence. Without structural independence, achieving independence of DPAs will only continue to remain a mirage. GDPR was unequivocal in this respect where it provides that the supervisory authorities must 'remain free from external influence, whether direct or indirect, *and shall neither seek nor take instruction from anybody*'.¹²⁰

The broad functions DPAs are expected to perform mean they need adequate resources. Independence also means that DPAs have sufficient manpower and financial resources. This is a big challenge that many DPAs are facing in Africa. For example, in a recent status report before the National Assembly, the Information Regulator of South Africa complained

117 As above.

118 Uganda Data Protection and Privacy Act sec 4(1).

119 'Mandate', <https://nitda.gov.ng/mandate/> (accessed 1 September 2021).

120 GDPR art 52(2).

of limited funds. In fact, she further complained of lack of a permanent office space.¹²¹ Similarly, it was reported that in the 2018/2019 financial year, the South African Information Regulator had to work with a budget of R27 Million, which was the same amount expected in the next financial year when the Regulator is supposed to be fully operational.¹²² Besides, the Regulator must also combine the task of overseeing the enforcement of the POPIA with the Protection of Access to Information Act.¹²³ According to Adam and Adeleke, this is a 'woefully low budget' compared to similar independent institutions such as the South African Human Rights Commission.¹²⁴ The Mauritius Data Protection Commissioner also made a similar remark regarding insufficient human resources, which could impede the effective enforcement of the Data Protection Act. According to the Data Protection Commissioner, 'one longstanding problem faced by this office is the severe insufficiency of human resources, which inevitably hampers the efficiency of service delivery'.¹²⁵ This comment was made in the 2018 report. Unfortunately, this situation remained the same as reported in 2019. According to the Data Protection Commissioner, '[o]ur last annual report 2018 showed how this office struggled to meet service delivery due to a severe shortage of human resources. In 2019, the situation worsened since our workforce was reduced by two for better career options.'¹²⁶

Financial independence, no doubt, is key to achieving real independence. In Africa, governments have used control over finances to undermine the independence of statutory bodies, and this situation cannot be totally ruled out with regard to DPAs. In this regard, subsuming DPAs into ministries will pose a challenge to financial independence. According to Gbenga Sesan, '[i]f you get your money directly from the

121 SA Human Rights Commission Annual Report; Information Regulator Status Report, <https://pmg.org.za/committee-meeting/25227/> (accessed 1 September 2021).

122 R Adams & F Adeleke 'Protecting information rights in South Africa: The strategic oversight roles of the South African Human Rights Commission and the Information Regulator' (2020) 10 *International Data Privacy Law* 157, citing Dommissee Attorneys 'POPI News: Appointment of the Information Regulator' 7 November 2016, <http://dommisseeattorneys.co.za/blog/pop-news-appointment-information-regulator/> (accessed 1 September 2021).

123 As above.

124 As above.

125 Makulilo (n 97) 18, citing Data Protection Office Annual Report 2018.

126 Data Protection Office Annual Report 2019 9, <https://dataprotection.govmu.org/AnnualReports/DPO%20Annual%20Report%202019.pdf> (accessed 1 September 2021).

national budget, you have more power. If you get your money from the ministry, you have no power.’¹²⁷

The absence of a specific data protection supervisory body at the regional level may also have direct or indirect implications for the establishment and guarantee of independent DPAs. Looking at the structure that exists in the EU, it will be seen that the role of the supervisory agency at the regional level, the European Union Data Protection Supervisor (EDPS),¹²⁸ is significant in pushing for independence at the domestic level.¹²⁹ Similarly, the newly established European Union Data Board (EUDB) is responsible for regional harmonisation and has proactively led DPAs in the EU toward effective data protection enforcement.¹³⁰ The office of the supervisor has been proactive in ensuring that member states fulfil their obligations under GDPR. There are numerous cases initiated or supported by the EDPS member states for not complying with provisions on independence. For example, in cases such as *Commission v Hungary*¹³¹ and (*Grand Chamber*) *European Commission v Republic of Austria*,¹³² member states were brought

127 Quoted from Davis (n 104) 53.

128 EDPS ‘About us’, https://edps.europa.eu/about/about-us_en (accessed 1 September 2021).

129 L Jančiūtė ‘European Data Protection Board: A nascent EU agency or an “intergovernmental club”?’ (2020) 10 *International Data Privacy Law* 57-75.

130 See A Giurgiu & TA Larsen ‘Roles and powers of national data protection authorities’ (2016) 2 *European Data Protection Law Review* 342-352. See also EDPB ‘Who we are’, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (accessed 1 September 2021).

131 Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237 8 April 2014, also available online at European Union Data Protection Supervisor (EDPS). In brief, the decision of the Court with regard to independence was that ‘by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data, Hungary has failed to fulfil its obligations under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data’.

132 See Case C-614/10, CJEU (Grand Chamber) *European Commission v Republic of Austria*, 16 October 2012, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0614&from=EN> (accessed 1 September 2021). Briefly, the Court was of the view that by failing to take all measures necessary to ensure that the legislation in force in Austria meets the requirements of independence with regard to the Data Protection Commission, more specifically by making a regulatory framework that makes the Data Protection Authority integrally linked to the Federal Chancellery, the Republic of Austria has failed in its obligations under art 28(1) of the EU Directive which requires ‘complete independence’ of DPA. For a more in-depth analysis of this decision, see A Balthasar ‘Complete independence of national data protection supervisory authorities – Second try: Comments on the judgement of the CJEU of 16 October 2012, C-614/10 (*European Commission v Austria*)’, with due regard to its previous judgment of 9 March 2010, C-518/07 (*European Commission v Germany*)’ (2020) 9 *Utrecht Law Review* 26-38.

before the Court of Justice of the EU for failure to comply with the requirement of independence. Although the nature of supranationalism that exists under the African Union (AU) is incomparable to that of the EU, a regional data protection body will go a long way towards assisting state parties. While the AU Commission is making some effort to be this regional body,¹³³ such effort cannot be compared to having a body that focuses on data protection alone.

Still within the regional context, networks of data protection authorities have been instructive in expanding the understanding of independence. They do this by having certain accreditation requirements for DPAs of member states. While there is one such network in Africa, the Network of African Data Protection Authorities, it appears that they have not developed an accreditation criterion. The website of the network merely provides that its membership is limited to 'data protection authorities in states which have adopted legislation on privacy and data protection'.¹³⁴

It needs not be gainsaid that achieving independence in typical African countries will be a struggle for several reasons. Even in Europe where the concept seems to have developed, it constantly is under threat.¹³⁵ However, African countries present peculiar challenges, as mentioned above.

5 Conclusion

The essence of this chapter is to analyse the international standards on independence of data protection authorities and the extent to which they have been applied in Africa. The chapter also sought to identify the possible hurdles that DPAs may face in achieving independence from a broader context. Indeed, without independence, a DPA operates like a paper tiger. Similarly, despite the initial controversies regarding the 'one-size-fits-all application of the concept', it seems to now be settled that the independence and effectiveness of a DPA are intricately linked. As rightly noted, 'there is a clear link between DPA independence and the

133 Examples of such efforts by the AU Commission include the issuance of the Personal Data Protection Guidelines for Africa that were made pursuant to the AU Convention. It is a joint initiative of the Internet Society and the Commission of the African Union, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 1 September 2021).

134 Network of African Data Protection Authorities 'Becoming a member or observer', <https://www.rapdp.org/en/devenir-membre-observateur> (accessed 1 September 2021).

135 P. Schütz 'Assessing formal independence of data protection authorities in a comparative perspective' in J. Camenisch and others *Privacy and identity management for life* (2011) 45.

impartiality and integrity of compliance and enforcement schemes that go beyond traditional governmental regulatory structures'.¹³⁶ While there is a difference between formal/legal independence and independence in practice, I argued that the former is crucial for a realisation of the latter. That is why the focus essentially was on an analysis of statutory provisions on independence on the continent, and future research will do well to consider the practical perspective of the topic. GDPR currently provides the most exhaustive stipulation on independence and, owing to its influence and globalising effect, it appears that those standards will be the next international metric against which independence of DPA will be assessed.

At the regional level, the ECOWAS Supplementary Act provides the most detailed provisions on independence, albeit with lapses. The AU Convention is vague in this respect and the Personal Data Protection Guidelines for Africa that were recently issued by the AU Commission add nothing significant in putting flesh to the Convention toward a better understanding. The approach to regulatory independence at the domestic level has not been good. Most African countries make very vague stipulations on independence with some not even making any provision. In practice, the DPAs of many countries have been made subject to an overwhelming supervisory role of key ministries of government, thereby significantly affecting their independence. Only the South African POPIA makes a laudable provision in this regard on the continent. Not only is the stipulation very detailed, but it could arguably also stand the test of GDPR. It is therefore recommended that future reforms of data protection regimes in other countries could take a lesson or two from the approach of South Africa.

Another area other countries could learn from South Africa is regarding the method of establishment of certain statutory bodies called 'state institutions supporting constitutional democracy' under Chapter 9 of the South African Constitution.¹³⁷ The uniqueness of these institutions is the approach of entrenching them in the Constitution. Although the Information Regulator is not among those bodies, it is arguably designed to be like them. As mentioned in POPIA, the Information Regulators, like these institutions, are 'independent, and subject only to the Constitution and the law, and they must be impartial and must exercise their powers and

136 Cate and others (n 1) 2.

137 These are (a) the Public Protector; (b) the South African Human Rights Commission; (c) the Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities; (d) the Commission for Gender Equality; (e) the Auditor-General; and (f) the Electoral Commission.

perform their functions without fear, favour or prejudice'.¹³⁸ The uniqueness of these bodies is that the very act of constitutional entrenchment insulates them from undue politics and political interference. This has been argued to be one of the most effective means of guaranteeing the independence of certain statutory bodies.¹³⁹ African countries must, therefore, learn from this approach and probably consider constitutionally entrenching the roles and functions of DPAs in future constitutional reforms. However, given the difficulty of obtaining constitutional reforms, African countries can start by adopting the South African approach in section 39(b) of the POPIA in future reforms of their data protection legislation.

138 The Constitution of the Republic of South Africa, 1996 sec 181(2). The same provision is contained in POPIA sec 39(b).

139 Fombad (n 116) 325-344.

References

- Abdulrauf, LA ‘Giving ‘teeth’ to the African Union towards advancing compliance with data privacy norms’ (2021) 30(2) *Information & Communications Technology Law* 87
- Abdulrauf, LA & Fombad, CM ‘The African Union’s data protection Convention 2014: a possible cause for celebration of human rights in Africa?’ (2016) 8(1) *Journal of Media Law* 67
- Adams, R & Adeleke, F ‘Protecting information rights in South Africa: the strategic oversight roles of the South Africa Human Rights Commission and the Information Regulator’ (2020) 10(2) *International Data Privacy Law* 146
- Adepetun, A ‘Nigeria Data Protection Bureau awaits NASS on Startup bill’ *The Guardian* 9 February 2022. Also available online at <https://guardian.ng/technology/fg-creates-nigeria-data-protection-bureau-awaits-nass-on-startup-bill/> (accessed 9 April 2022)
- Birnhack, MD ‘The EU Data Protection Directive: An engine of a global regime’ (2008) 24(6) *Computer Law & Security Review* 508
- Data Protection Africa ‘Mapping 55 African countries | 36 data protection laws | 3 draft laws <https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf> (accessed 3 March 2024)
- Davis, T ‘Data protection in Africa: A look at OGP member progress’ <https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf> (accessed 1 September 2021)
- Fombad, CM ‘The role of hybrid institutions of accountability in the separation of power scheme in Africa’ in CM Fombad (ed) (2016) *Separation of powers in African constitutionalism* OUP: Oxford
- Flaherty, D (1987) *Protecting privacy in surveillance societies* University of North Carolina Press: North Carolina
- Greenleaf, G ‘Independence of data privacy authorities (Part I): International standards’ (2012) 28 *Computer Law & Security Review* 1
- Greenleaf, G ‘Independence of data privacy authorities (Part II): Asian-pacific experience’ (2012) 23 *Computer Law and Security Review* 121
- Greenleaf, G & Cottier, B ‘International and regional commitments in Africa data privacy laws: A comparative analysis’ (2022) 44 *Computer Law and Security Review* 1
- Giurgiu, A & Larsen, TA ‘Roles and powers of National Data Protection Authorities’ (2016) 2(3) *European Data Protection Law Review* 342

- Hoofnagle, CJ ; van der Sloot, B & Borgesius, FZ 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65
- Ilori, T 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solution' https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf (accessed 1 September 2021) 1
- Jančič, L 'European Data Protection Board: a nascent EU agency or an 'intergovernmental club'? (2020) 10(1) *International Data Privacy Law* 57
- Kuner, C; Cate, FH; Millard, C & Svantesson, DJ 'The intricacies of independence' (2012) 2(1) *International Data Privacy Law* 1
- Lynskey, O "The 'Europeanisation' of data protection law" (2017) 19 *Cambridge Yearbook of European Legal Studies* 257
- Makulilo, AB 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78
- Makulilo, AB 'The context of data privacy in Africa' in AB Makulilo (ed) *African Data Privacy Laws* (2016) Springer: Switzerland
- Makulilo, AB 'The GDPR implications for data protection and privacy protection in Africa' (2017) 1(2) *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 12
- Makulilo, AB 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25(1) *The International Journal of Human Rights* 133-134
- Merriam-Webster Dictionary online. <https://www.merriam-webster.com/dictionary/independent> (accessed 1 September 2021)
- Network of African Data Protection Authorities 'Becoming a member or observer' <https://www.rapdp.org/en/devenir-membre-observateur> (accessed 1 September 2021)
- Roos, A 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* 1
- Stein, P 'South Africa's EU-style Data Protection Law' (November 2012) *Without Prejudice* 48 available <https://journals.co.za/doi/pdf/10.10520/EJC128763> (accessed 1 September 2021)

- Schütz, P 'Assessing formal independence of data protection authorities in a comparative perspective' in Camenisch, J; Fischer-Hübner, S & Rannenberg, K (2011) *Privacy and Identity Management for Life* Springer: Berlin
- Tarasova, E 'Data protection authorities in Central and Eastern Europe: Setting the research agenda' in P Jonason & Rosengren, A (eds)(2017) *The right of access to information and the right to privacy: A democratic balancing act* Södertörn University Publications: Stockholm
- Zerstick, T 'Article 52. Independence' in Kuner, C; Bygrave, LA; Docksey, C & Drechsler, L (eds) (2020) *The EU General Data Protection Regulation (GDPR): A commentary* Oxford University Press: Oxford