MAKING ICT POLICY IN AFRICA

An Introductory Handbook

By Sekoetlane Phamodi (Ed.), Michael Power and Avani Singh

FRIEDRICH
EBERT
STIFTUNG

MAKING ICT POLICY IN AFRICA

AN INTRODUCTORY HANDBOOK

Published by *fesmedia* Africa
Friedrich-Ebert-Stiftung (FES)
P O Box 23652
Windhoek, Namibia
Tel: +264-61 417 523
Email: info@fesmedia.org
www.fesmedia-africa.org

Editor: Sekoetlane Phamodi

Authors: Sekoetlane Phamodi, Michael Power, Avani Singh

Cover photographs by @Townhouse Media

The findings, interpretations and conclusions expressed in this volume do not necessarily reflect the views of the FES or *fesmedia* Africa. *fesmedia* Africa does not guarantee the accuracy of the data included in this work.

ISBN: 978-99945-77-89-7

CONTENTS

CHAPTER 1: ICT GOVERNANCE FRAMEWORKS

CHAPTER 2: THE DIGITAL ECOSYSTEM

CHAPTER 3: RIGHTS AFFECTED BY ICT POLICY MAKING

APPENDIX 1: ICT POLICY CHECKLIST

APPENDIX 2: USING THE HANDBOOK AS A TRAINING RESOURCE

APPENDIX 3: RECOMMENDED RESOURCES

LIST OF ACRONYMS

4IR	Fourth Industrial Revolution
ACDEG	African Charter on Democracy, Elections and Governance
ACHPR	African Commission on Human and Peoples' Rights
ACRWC	African Charter on the Rights and Welfare of the Child
AfriNIC	African Network Information Centre
AU	African Union
ANZ	Associated Newspapers of Zimbabwe
CSO	Civil Society Organisation
DNS	Domain Name Systems
EAC	East African Community
EACJ	East African Court of Justice
ECOWAS	Economic Community of West African States
EU	European Union
GDPR	General Data Protection Regulation 2016/679 of the European Parliament and of the Council
GSMA	Groupe Spéciale Mobile Association
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IGF	Internet governance forum
IP	Internet protocol
ISP	Internet service provider
ITU	International Telecommunication Union
NEPAD	New Partnership for Africa's Development
NGO	Non-Governmental Organisation
OTT	Over-the-top service
SADC	Southern African Development Community
SDG	Sustainable Development Goal
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
VoIP	Voice over Internet protocol

GLOSSARY OF KEY TERMS

Anonymity	Acting or communicating without using or presenting one's name or identity, or as acting or communicating in a way that protects the determination of one's name or identity, or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity. Anonymity refers to taking no name at all, while pseudo-anonymity refers to taking an assumed name.
Blocking of content	Preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist.
Communications surveillance	The monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present or future.
Connectivity	The ability to use an electronic network in order to send and receive information between any locations, devices or networks.
Convergence	The way in which computing, telecommunications and broadcasting are moving towards a common technological basis characterised by the use of digital systems.
Critical information infrastructure	ICT systems, data systems, databases and networks that are fundamental to the effective operation of a state, particularly in relation to critical services such as the economy, social services and law enforcement.
Cybercrime	A crime that is committed using a computer network or the Internet.
Cybersecurity	The practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents, and responding to and recovering from them.
Digital divide	The perceived growing gap between those who have access to and the skills to use ICTs, and those who, for socio-economic and/or geographical reasons, have limited or no access.
Digital literacy	The ability to use digital technology, communication tools or networks to locate, evaluate, use and create information.
e-Government	The use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and government itself.
Encryption	A mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient and, in doing so, protects the confidentiality and integrity of content against third party access or manipulation.
Filtering of content	Making use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful.
ICT	Any technology used for the processing, communication and manipulation of information.

Information society	A society in which the creation, distribution and manipulation of information has become the most significant economic and cultural activity.
Inter-operability	Devices in particular application programmes that, in addition to communicating with each other, can also cooperate and execute a common task together.
Intermediary (or Internet intermediary)	An entity which provides services that enable people to use the Internet, falling into two categories: (i) conduits, which are technical providers of Internet access or transmission services; and (ii) hosts, which are providers of content services, such as online platforms and storage services.
Intermediary liability	Liability incurred by an intermediary where governments or private litigants can hold technological intermediaries, such as ISPs and websites, liable for unlawful or harmful content created by users of those services.
Internet protocol	A network-layer protocol that contains addressing information and some control information that enables packets of data to be routed between hosts on the Internet.
Internet service provider	An organisation, such as a company, that provides subscribers with access to the Internet.
Internet shutdown	An intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.
Network neutrality	The principle that all Internet data should be treated equally without undue interference, and promotes the widest possible access to information.
OTT	An application or service that provides a product over the Internet and which bypasses traditional distribution; it includes, for instance, Facebook or WhatsApp.
Personal information (or personal data)	Any information relating to an identified or identifiable natural person (referred to as the data subject), whereby that data subject can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.
Spectrum	The radio frequencies allocated to the mobile industry and other sectors for communication over the airwaves.
Universal service fund	Fund or contribution paid by telecommunications operators, typically in the form of a percentage of revenue, to fund projects that increase access to telecommunications services in the country of operation.
VoIP	The transmission of voice and multimedia content over the IP networks; it includes, for instance, Skype.
Zero-rating	The practice of providing Internet access without financial cost, subject to certain conditions, such as by only permitting access to certain websites or by subsidising the service with advertising.

PREFACE

In the digital age, the development and effective implementation of Information and Communication Technology (ICT) policies is critical for countries to harness the full potential of ICTs in driving inclusive and sustainable development, by promoting universal access to information, internet universality, good governance, e-commerce, equitable quality education, among other important enablers of social and gender justice and socio-economic development. It is argued that globally, the digital divide is widening between the digital "haves" and the digital "have-nots" and closing the gaps - locally, nationally and globally requires creative pro-people policies that focus on national priorities, on areas that will have a positive impact on people's lives. This is especially true for the African context where the need for robust, pro-people ICT policies is evident.

At fesmedia Africa, we believe that all citizens, including women, youth and the marginalised must be empowered to be able to participate meaningfully in decision- making and democratic debate and to contribute to the economic, social and political progress of their societies and countries. For this to happen, citizens need to have the means, skills and opportunities to access, exchange and use information and knowledge through the utilisation of ICTs. In this regard, we believe that countries should develop robust ICT policies and facilitate the effective deployment of ICTs in order to strengthen the information and communication environments, which is a prerequisite for functional, participatory democracies.

This handbook was developed to facilitate and contribute to ongoing efforts towards the development of ICT policies in Africa and it seeks to enable a greater number of citizens to participate in this important endeavour. It provides a detailed explanation of ICT policy, why ICT policy matters and guiding principles for ICT policy drafting. It is a reader friendly, easy-to-follow introductory guide to ICT policymaking in Africa, based on in-depth analysis of the impact of ICT on the continent and the need for principles to guide its development, deployment and use. The handbook provides users with overarching principles, good practices and strategies that can be applied in different contexts. It includes a knowledge check and is well cited, which makes it valuable as a training resource.

We sincerely hope that this guide will be beneficial for any and all wishing to contribute to the development and implementation of effective and progressive ICT policies in Africa. Or those simply wishing to have an understanding of the issues involved.

I wish you happy reading.

Freya Gruenhagen, Director, *fesmedia* Africa

INTRODUCTION

The emergence and ubiquity of information and communication technologies (ICTs) has had a profound impact on almost all areas of public and private life. From facilitating communication and information-sharing, increasing access to educational opportunities, ensuring better access to government services, and enabling business opportunities, these technologies have accelerated human development and improved the quality of people's lives in incalculable ways.

The concept of ICTs is a generic term that describes the general processing and communication of information through technology. This includes, for instance, radio, television, cellular phones, computer and network hardware and software, satellite systems, as well as the various services and applications associated with them, such as social media, video-conferencing and distance learning. ICT policy, in turn, seeks to regulate the access to and use of ICTs. It is essential that, as the role played by ICTs continues to expand, ICT policies are designed in a manner that is informed, rights-based and technologically appropriate, and that barriers – including cost, access, infrastructure and capacity – are addressed.

This introductory handbook to the development of ICT policy in Africa aims to assist law makers, government officials, lawyers, civil society organisations (CSOs), academics and members of the public engaged in the development and implementation of ICT policy. Its primary purpose is to provide an introductory overview of the fundamental concepts and regulatory issues emerging in the process of ICT policy making, and to introduce good practice models for how to approach both the process and the issues as they emerge. Recognising that ICT policy making is a complex and developing subject area, this handbook is not an exhaustive resource. It is an introductory guide to support the user in finding their feet in fast-paced and often overwhelming field so that they can participate meaningfully in ICT policy making processes as they also develop their knowledge through further research and direct experience.

This handbook seeks to provide users with the overarching principles, good practices and strategies that can be applied in a multitude of circumstances. It may also be used as a training resource. In particular, Appendix 2 provides practical exercises and resources which can be completed in both self-managed as well as facilitated learning contexts to help users of this handbook apply theory to real-world ICT governance problems.

The handbook is structured as follows:

- **Chapter 1: Governance frameworks and why they matter** frames a conceptual understanding of what constitutes ICT policy. It distinguishes between different legal instruments and how they interact with one another to form the ICT governance framework. It further provides an overview of the main imperatives driving ICT policy development.
- **Chapter 2: The digital ecosystem** introduces the layer model of the Internet in order to frame a conceptual understanding of the digital ecosystem. It provides a conceptual understanding of what functions and relationships ICT policies typically govern, as well as identifies which key role players are involved in the development of ICT policy, and their respective and inter-related functions.
- **Chapter 3: Rights affected by ICT policy making** sets out which rights are most directly impacted by ICT policies and how. It considers the public international law implications for how ICT governance frameworks are developed. It reflects on some of the most significant legal challenges and debates concerning human rights and the Internet. Lastly, it considers some existing principles and instruments for how domestic and public international law has been applied to selected ICT governance and human rights problems in Africa.

- **Chapter 4: ICT policies in practice** offers an overview of the guiding principles underpinning the ICT development process – from formulation to implementation. It outlines and describes the most significant steps in the ICT policy making cycle. It draws on the lessons learned in policy development processes in various countries in the region and further abroad, providing comparative analyses and good practice guidelines, with particular reference to African examples.

This is supplemented by the following appendices (tools) at the end of the handbook:

1. **Appendix 1: ICT policy checklist** is for assisting policy-makers and other stakeholders in the formulation and implementation of ICT policies to reflect on whether and how each of the steps in the ICT policy making process have been adequately followed.
2. **Appendix 2: Using the handbook as a training resource** sets out various tools and exercises to support users in self-driven or guided learning to apply the theory and concepts discussed in this handbook to real-world ICT policy making problems. It prompts discussion on various policy issues explored through this handbook, and contains a quiz to test users' knowledge.
3. **Appendix 3: Recommended resources** sets out a list of strongly recommended resources that can be used for more information, or in the structuring of a training session or programme.

Lastly, we note that the field of ICT policy is dynamic and rapidly evolving. While every effort has been made to ensure that the information is correct at the time of publication, new developments constantly occur.

CHAPTER 1 ICT GOVERNANCE FRAMEWORKS AND WHY THEY MATTER

OBJECTIVES OF CHAPTER 1

In this chapter we will:

- Frame a conceptual understanding of what constitutes information and communication technology (ICT) policy.
- Distinguish between different legal instruments and how they interact with one another to form the ICT governance framework.
- Provide an overview of the main imperatives driving ICT policy development.

1.1 What exactly is ICT policy?

The term 'ICT policy' generally refers to a wide range of different policies that impact on the access and use of ICTs. This can include, for example, a broadband policy which sets out the framework and standards for how broadband infrastructure in a country should be rolled out, accessed and used. It can also include an e-government policy, which sets out how government services should be made accessible online, or a cyber-security policy which defines the measures and procedures by which public assets and infrastructure can be protected against malicious cyber-attacks.

Traditionally, ICT policies have typically dealt with four broad categories of ICT-related matters:[1]

- Computing and information technology.
- Broadcasting, including radio and television.
- Telecommunications, including telephony and data communications through fixed and wireless networks.
- The Internet and Internet-related services.

However, as innovation progresses and network technology continues to fundamentally shape how society is organised, the scope of ICT policy expands beyond the ICT sector itself and the services it offers, and intersects with and influences other areas of public policy.

In practice, ICT policy can take different forms depending on the public institution enacting it. Broadly speaking, a country's policy positions on ICT matters is articulated in the combination of the laws enacted by the legislative sphere of government, the policies and proclamations enacted by the executive sphere, as well as the regulatory instruments enacted by specifically designated bodies such as market or communications regulators.

At the outset, it is important to distinguish between legislation, policies and regulations as *legal instruments,* each of which are enacted by different bodies or authorities, and which are different in the scope of their mandates, application and enforceability. Being able to distinguish between these instruments, the political processes and mechanisms by which they are enacted as well as how they interact with one another, is key to being able to participate meaningfully and effectively in ICT policy making.

[1] Association for Progressive Communications (ACP). 2009, 'The APC ICT Policy handbook', p7. Accessible at https://www.apc.org/sites/default/files/APCHandbookWeb_EN_0.pdf.

1.1.1 Policy

Policy is usually a good place to begin because this is the legal instrument which often precedes legislation. Policies represent the *intention* of a government, providing a *deliberate plan* of action which *guide decisions* and *structural arrangements* to produce a *rational outcome*. They are usually enacted by the executive arm of government through a participatory process to define the outcomes the named implementing authorities should be working to achieve, as well as guidelines for how to do so within the parameters set out in existing or new legislation. Such policies may provide context, set out the country's intended commitments, and identify strategies for achieving those commitments.

Policies are usually aspirational in nature and, typically, do not have legally binding implications. Nevertheless, because they form the rational basis for government action and are ideally defined through a democratic process, there has to be a corresponding link between the policy statement and those legally binding laws and regulations which flow from it, or within which it operates. A policy may be accompanied by supporting documents, such as a strategy, implementation plan or a roadmap.

1.1.2 Legislation

Legislation is enacted by the parliament of a country, and constitutes binding law. It typically sets out the body of role players responsible for performing a specific function, the rules and procedures to be followed in doing so, and the enforceable rights and remedies available to affected parties.

Legislation and policies must be mutually supportive and should, therefore, be developed and implemented in a reasonable and rational manner, meeting the rights-based standards set in the country by constitutional provisions and international human rights law. For ICT laws and policies, because they substantially impact on information and communication rights, the rights to freedom of expression, access to information, privacy and equality are of particular importance.

1.1.3 Regulation

Regulations are often written to implement the specifics of a particular law, such as providing for a licensing framework, or practically operationalising clearly defined policy objectives. They are promulgated in terms of legislation to define rules and procedures that must be followed by regulatory authorities and rights-bearing role players in their interactions with one another. They set out the technical conditions under which action may be taken by the designated authority, as well as the considerations which should guide the decisions that may be taken by that authority.

Because they directly impact the rights and legally recognised expectations of these role players, regulations are not only enforceable, but require public participation in their development and amendment. However, regulations do not typically have to go through the full parliamentary process, although they must still comply with the rights-based standards set in the country in which they operate. They will usually be developed and enforced by an authority such as a Minister or designated regulatory authority in line with existing legislation governing their subject of regulation. The totality and interactions between these instruments and bodies is what is broadly understood as the *ICT governance framework*.

In this handbook the focus will primarily be placed on ICT policy. This is because policies are the primary site for negotiating, contesting and defining detailed information about the intent of government, in consultation with rights-bearers, to produce clearly defined rational outcomes, the measures required to produce them, and the steps that will be taken to implement them.

Notwithstanding, some substantive aspects discussed in this handbook may be found in different legal instruments in different countries, depending on the approaches they take in defining their ICT governance framework and the political processes through which their governance systems are organised. Although the status of the law may differ depending on which legal instrument is relied upon, the overarching considerations, principles and strategies remain equally applicable.

1.2 Why do ICT policies matter and to whom?

ICTs, which include the Internet, are transforming how society is organised. In all their forms, they are powerful tools in facilitating the gathering and transmission of information and ideas between persons, for delivering goods and services, as well as for facilitating effective governance and service delivery. The impact of ICT policy on all areas of life is far reaching, making it all the more important for all aspects of society to not only be interested in, but be actively involved in the decision making processes and mechanisms through which ICT policy is developed.

For most people, their primary interaction with ICTs and ICT policy is at the level of their ability to access information and share their ideas freely with one another, mainly through the Internet. The United Nations Educational, Scientific and Cultural Organization (UNESCO) describes the profound impact the Internet has had on societies as follows:[2]

> *Probably the single most important factor in understanding the impact of the Internet on freedom of expression is the way in which it increases our ability to receive, seek and impart information. It enables the collaborative creation and sharing of content – it is a world where anyone can be an author and anyone can publish. The Internet is helping develop spaces that can empower people, helping them communicate, collaborate and exchange views and information.*

So, whether by e-mail, websites or social networking platforms, people are more closely connected and better equipped for instant sharing of huge and diverse amounts of information, across borders, and with wide audiences. They are better enabled to engage with diverse views and perspectives, and to access an array of resources that enable them to formulate their own views.[3] What this widespread availability of information has meant is that there is no longer any one source for truth or valid perspective by which people can be informed. Further, because the means of publishing are now more readily available, both information and expression are now more substantially democratised, and it is no longer necessary to look to the professions and institutions traditionally regarded as authorities or gatekeepers of that information to get access to it or act as public spokespeople for our views.

But the global impact of ICTs extends much further than its role in respect of information and communication rights. ICTs have, in many ways, become central to everyday life. They are intrinsic to everyday services that people rely on, such as banking, and in the provision of fundamental government services, such as the provision of social assistance grants or payment of income tax. These kinds of everyday services require reliable and secure infrastructure and channels of verification in order for both the state actors and people to trust and use them to make their lives easier and better.

In connecting people closer together than ever before, and enabling them to impart information and ideas, ICTs have also had the impact of strengthening democratic processes, as well as meaningful participation in governance and decision making. The availability of public information such as budget

[2] UNESCO. 2016a. *Freedom of Expression and the Internet*. Montevideo: UNESCO. Accessible at: http://unesdoc.unesco.org/images/0024/002466/246670e.pdf.

[3] Media Legal Defence Initiative. 2018. *Training Manual on Digital Rights and Freedom of Expression Online*. London: Media Legal Defence Initiative, 4. Accessible at: https://www.mediadefence.org/resources/mldi-training-manual-on-digital-rights-and-freedom-of-expression-online/.

and public audit data in electronic form, for example, has also built more transparent, efficient and inclusive relationships between governments and citizens. ICTs enable governments to leverage data in how they respond to the biggest social problems of the day, and citizens are better equipped to advocate for their rights from an informed position, having had sight of the same evidence governments are relying on to drive their programmes.

While most governments recognise the benefits of ICTs for good governance and social development, there are also those that remain wary of the role that ICTs can play in destabilising ineffectual and, sometimes, undemocratic governance systems. In these contexts, ICT policies have taken the turn of imposing content or access restrictions that may unduly encroach on the rights to freedom of expression, access to information or privacy. Such policies are unfavourable to realising the full potential that ICTs can offer.

Because of how far reaching the impact ICTs can have on these and other aspects of social interaction, governance and development, it is apparent that a wide range of sectors, industries and role players in both the public and private sector stand to be affected by the ICT policies that form part of the relevant legal framework. Everyone has a stake, making it all the more important that ICT policies are developed in a rights-based manner that strikes the appropriate balance between competing rights and interests.

1.3 What kinds of imperatives do ICT policies respond to?

ICT policies and other related legal instruments are developed to respond to a variety of issues. For example, in recent years across the region, we have been seeing a turn to rhetoric concerning the Fourth Industrial Revolution or "4IR". It has been mobilised to signal a fundamental and comprehensive shift in the structure of social participation and economic productivity in which technology and the Internet are at the centre. Major discussion points under this theoretical framework have included everything from how the state and governments should approach the digitalisation of government services and leverage its access to large data sets in order to enhance the quality of service to citizens, through to how we imagine and prepare for the future of work in a context where technology is evolving very quickly, and in ways in which it is able to perform the same kinds of tasks humans do at a greater speed and with more precision.

Whatever we call them, the major technology driven shifts to public and private life we are observing and preparing for today are raising some fundamental public policy debates which have become the very object of ICT policy making. Regardless of the complexity of the issues we might be responding to in the course of the policy development process, however, we can safely understand the concern of ICT policy making to respond to three key purposes as follows:

- **Infrastructure coordination and technical standardisation.** This establishes a common and legally enforceable platform for all businesses within a sector or across the whole of business. This can be managed at the global, regional or national level through standards agencies.
- **Market regulation.** This seeks to create and maintain fair competitive market conditions and relationships between businesses, as well as between businesses and consumers. In the ICT sector they can cover a range of issues from diversifying ownership and control dynamics in the sector to establishing pricing controls over certain ICT goods and services.

However, how they get onto the policy agenda in the first place can vary substantially. These policy programmes may be introduced by government itself, having reviewed the prevailing governance framework against its mandated programmes or, as is usually the case, in response to advocacy and engagement by citizens, including the private sector, drawing attention to the problems they are facing, and how policy intervention can respond to them.

Through the development of **appropriate**, **relevant** and **people-centred** ICT policies, measures can be put in place to make significant gains in delivering universal and comprehensive access to the global information society. This can further promote the use of ICTs to achieve social and economic inclusion, as well as deepen the enjoyment of human rights and democratic governance.

To achieve this does not necessarily require more regulation. It requires effective regulation that appropriately harmonises existing regulatory frameworks domestically, regionally and internationally, and which addresses the new competitive paradigm brought about by the knowledge economy. It also accepts the need for collaborative regulation between other sector regulators.[4]

Below we consider some of the main imperatives which drive ICT policy development, and some of the key considerations that must be taken in the processes and mechanisms that produce them:

- Sustainable human development.
- Stimulating economic growth.
- Securitisation.

1.3.1 Sustainable human development

It is well documented how well crafted ICT policy can facilitate participation in the global information society by leveraging knowledge for sustainable development.[5] Detailed ICT policy frameworks that are appropriately tailored to the needs of the local context can encourage investment in ICT infrastructure and facilitate the introduction of better services to consumers.[6] They can also stimulate sustainable socio-economic growth. Well-crafted ICT policies can enable effective regional coordination in the creation of larger markets, open up access to new markets, as well as allow direct, simultaneous and decentralised collaboration, advocacy, trade, production, and innovation.[7]

The primary outcome of good ICT policy should be to enable universal service and access to ICTs, and ensure that every person can enjoy the benefits and opportunities that ICTs can offer.[8] In reality, however, governments will be required to balance this against other competing considerations, such as resource constraints, prevailing market dynamics, and regulatory value.

The current reality is that nearly half the world's population is not using the Internet or does not have the skills to make the best use of its connected technologies and services.[9] While access to ICTs can serve to increase opportunities, a major concern is that a lack of access can further entrench existing socio-economic divides. Bridging the **digital divide**, therefore, becomes a critical priority in the policy agenda for every country that is serious about rapidly equalising access to opportunity and participation in society and the economy in order to improve the lives of their people.

[4] ITU. 2018b. *Regulatory Challenges and Opportunities in the New ICT Ecosystem.* Geneva: ITU. Accessible at: https://www.itu-ilibrary.org/science-and-technology/regulatory-challenges-and-opportunities-in-the-new-ict-ecosystem_pub/81118c75-en.

[5] Chavula, H. & Chekol, A. 2010. ICT Policy Development Process in Africa. IJICTRDA. 1. 20-45. 10.4018/jictrda.2010070102.

[6] Mohamed, M.S. et. al. 2010. Information and Communication Technology (ICT) Policy: A Quantitative Assessment for Sustainable Development. *Journal of Information and Knowledge Management*.

[7] Kuyoro, S.O. 2012. ICT: an effective tool in human development. *International Journal of Humanities and Social Science*. 2(7):157-162.

[8] Gillwald, A. 2015. ICT4D, Regulation and Strategy. *The International Encyclopedia of Digital Communication and Society*: 1-11.

[9] ITU. 2019. Measuring Digital Development: Facts and Figures. Geneva: ITU: Accessible at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

THE DIGITAL DIVIDE

What is the digital divide?

The digital divide is the gap that exists between people who have access to modern ICTs and services, and those who do not have access to them. The term describes the substantial inequality this causes within and between populations whereby some parts of the population have substantially better access to opportunities to benefit from the new economy than others. This divide usually runs along the same lines as existing socio-economic inequalities within a population, as well as between countries.[10]

Digital inequality is most obviously evident between urban and rural populations, wealthy and poor communities, and between countries with more and less developed economies. It is also highly gendered as well as driven by the population's prevailing social arrangements whereby e.g. men, non-disabled persons and dominant racial, linguistic and cultural groups will enjoy greater and less restricted access to ICTs and the opportunities they offer than women, disabled persons or linguistic and cultural minorities.

At the level of structuring an Internet governance framework with the aim of narrowing socio-economic inequality and improving development outcomes for all, it is imperative for governments to institute measures which stimulate the bridging of the digital divide so as not to produce these inequalities in the new economic landscape.[11]

Areas of particular importance to focus on at the level of policy include:

- *Investing in supply-side interventions such as improved network infrastructure rollout and market regulation interventions which ease market access and stimulate competition.*
- *Lowering barriers to entry to consumer access to ICTs by encouraging affordable broadband services as well as the tools to connect, placing emphasis on the communities with the least access.*
- *Stimulating use of broadband services through demand-side interventions such as comprehensive digital literacy initiatives, investment in local and accessible content online, as well as incentivising online* participation of communities least likely to make use of the Internet to do so.

1.3.1.1 International recognition of the role of ICTs for sustainable development

The United Nations (UN) and its various structures, mechanisms and implementing agencies have expressed how ICTs can be marshalled to leapfrog some of the most persistent barriers to development and accelerate progress towards achieving its 17 goals for sustainable development.[12] SDG 9 in particular – *helping to build resilient infrastructure, promoting inclusive and sustainable industrialisation and fostering innovation* – expresses the particular significance of how efficient and affordable ICT infrastructure and services can enable countries to participate in the digital economy and increase their overall economic well-being and competitiveness.

In doing so, they can produce a substantial positive impact for their citizens in the areas of financial inclusion, poverty reduction, and improved health outcomes.

[10] Kuyoro, S.O. et. al. 159.

[11] Blimpo, M.P. et. al. 2017. *Leapfrogging: The Key to Africa's Development-from Constraints to Investment Opportunities*. Washington, D.C: World Bank Group. Accessible at: http://documents.worldbank.org/curated/en/121581505973379739/Leapfrogging-the-key-to-Africas-development-from-constraints-to-investment-opportunities.

[12] ITU. 2018a. *ICTs for a Sustainable World #ICT4SDG*. Geneva: ITU. Accessible at: https://www.itu.int/en/sustainable-world/Pages/default.aspx.

The African Union (AU) takes a similar view of ICTs as critical enablers for accelerating inclusive growth and sustainable development on the continent in its own strategic framework Agenda 2063: The Africa We Want.[13] This is expressed in the following aspirations:

- That cities and other settlements are hubs of cultural and economic activities, with modernised infrastructure, and that people have access to affordable and decent housing with all the basic necessities of life, including ICT.
- That the necessary infrastructure will be in place to support Africa's accelerated integration and growth, technological transformation, trade and development, including a well-developed ICT and digital economy.
- Under the call to action to connect Africa through world-class infrastructure, it provides that there should be a concerted push to finance and implement major infrastructure projects in, amongst others, ICT. In this regard, it envisions "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 […].

Effective ICT policy that is both aspirational and responsive to the prevailing development challenges of its context, therefore, becomes essential to ensure that ICTs can connect people to processes and opportunities in an inclusive manner that does not serve to deepen existing inequality.

1.3.2 Stimulating economic growth

There is good evidence for how the development of an ICT governance framework which invites digitisation and the digital economy can stimulate productivity and economic growth.[14] An International Communications Union (ITU) study[15] on the relationship between digitisation and economic growth in nine Latin American countries demonstrates the positive economic impact the introduction of coordinated regulation and institutions designed to stimulate the development of a digital economy can have for economic growth.[16] As can be seen in Illustration 1 below,[17] the study found that changes to the digitisation index growth, represented as compound annual growth, are directly related to changes in the institutional and policy environment. In each of the countries studied, changes to that institutional and policy environment were in the form of accelerated public investment in ICT infrastructure, increased efficiencies in the development of public policy initiatives, better coordination or increased efforts from the private sector aimed at investment and competitiveness, or a combination of these factors.

These gains are substantial, and can be directly attributed to the following key factors in the operational policy context and institutional arrangements:[18]

1. Developing a national digital agenda through a centralised authority with a clearly defined mandate enabled the coordination of public policy initiatives and the ability to build policy and legislative consensus efficiently.

[13] AU. 2013. Agenda 2063: *The Africa We Want.* (Popular version) Addis Ababa: African Union. Accessible at: https://au.int/en/Agenda2063/popular_version.

[14] Adeleye, N. & Eboagu, C. *Evaluation of ICT development and economic growth in Africa. Netnomics.* Accessible at: https://doi.org/10.1007/s11066-019-09131-6.

[15] ITU. 2018c. *The Economic Contribution of Broadband, Digitization and ICT Regulation* Geneva: ITU. 1. Accessible at: https://www.itu.int/pub/D-PREF-EF.BDR-2018.

[16] *Ibid.*

[17] *Ibid.*

[18] *Ibid*.

2. Accelerating public investment in ICT through sound policy instruments and fit-for-purpose institutions had the result of improving network reliability and affordability, and demonstrated the seriousness of the public sector in harnessing ICTs for economic growth.

3. By making these investments and introducing these institutional changes, the public sector was able to "signal" that ICT and digital development was a national development priority, thereby inviting accelerated private sector investment into the economy.

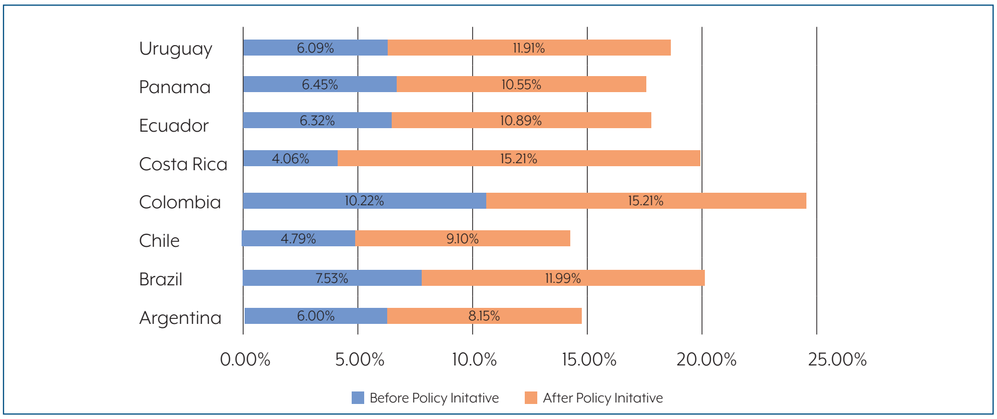

Illustration 1: Impact of political and institutional factors on rate of change on digitization index

Source: ITU, 2018c

The benefits should not be seen as unique to these Latin American countries. They typify how structured and coordinated approaches to the reorganisation of the ICT governance framework can play a significant role in stimulating growth and accelerating socio-economic development.

1.3.3 Securitisation

The protection of the state and society against digital threats and risks, such as cyber-attacks, has become a high priority on the national security agenda in many African countries. Consequently, most of the developments in ICT governance frameworks in the region have been predominantly approached through the lens of promoting cybersecurity and protecting national security. These initiatives have included the creation of sophisticated governmental cybersecurity agencies, the development of national cybersecurity strategies, and the enactment of cybercrimes legislation to introduce new formulations and penalties for technology-mediated conduct that can sometimes contradict established public policy principles.[19] Matters of cybercrime and cybersecurity tend to be constructed primarily as issues of national security – rather than as multi-dimensional and cross-cutting issues with technical, economic and political implications.

This is well demonstrated across many African states. There is a record of newly introduced cybercrime and cybersecurity frameworks directly conflicting with established legal norms, policies and standards. Some of these pose serious threats to human rights obligations. These have typically taken the form of new prohibitions and penalties for speech acts online that conflict with pre-existing criminal and civil law frameworks and remedies. Or the extension of new and unregulated powers of surveillance, search and seizure, as well as control over the functioning of network infrastructure to state authorities in the name of national security.

Governments have a responsibility to take measures to safeguard their national security imperatives against threats, and the cybernetic dimensions of these threats are no exception. However, caution must be exercised to ensure that this does not encroach on protected rights in an excessive or unjustifiable manner. Certainly, in addition to potentially violating citizens' rights and breaching public international

[19] Geelen, M. 2016. *Cyber securitization and security policy: The impact of the discursive construction of computer security on (national) security policy making in the Netherlands,* 1. Accessible at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/53654/2016_Geelen_CSM.pdf?sequence=1.

law in the name of pursuing legitimate aims, the development and adoption of excessive cybercrimes and cybersecurity legal instruments without regard to their interaction with the overarching ICT governance framework or aligning them with ordinary functioning of just administrative action and the rule of law may also have devastating consequences for investor sentiments and economic development.[20]

As has been previously noted by the Special Rapporteur on Freedom of Expression of the United Nations Human Rights Council:[21]

> *The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.*

As a general principle, the inclusion of and reliance on national security grounds in the development of ICT policy should not lead to the limitation of rights unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the stated threat. To this end, there is good guidance in public international law.

As explained in General Comment No. 34 in reference to article 19(3) of the Internet Covenant on Civil and Political Rights (ICCPR), extreme care must be taken by states to ensure that laws relating to national security, such as treason laws, are crafted and applied in a manner that conforms to the strict requirements of article 19(3); importantly, it is not compatible with article 19(3) for instance, to use such laws to suppress or withhold information from the public of legitimate public interest that does not harm national security, or to prosecute persons – such as journalists, researchers, activists or human rights defenders – for having disseminated such information.[22] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information also provide clear, human rights-respecting guiding principles concerning how national security frameworks and supporting legal frameworks can best be approached which are based on international and regional laws and standards, evolving state practice, and general principles of law recognised by states.[23]

The discussion on cybercrimes, cybersecurity and surveillance and how to approach it is dealt with in further detail in Chapter 3.

[20] CIPIT. 2018. International Internet Disruptions in Africa: Estimating Impact in Observable and Shadow Economies. Nairobi: Strathmore University. Accessible at: https://cipit.strathmore.edu/wp-content/uploads/2020/05/PDF-3.pdf; Iiori, T. & Killander, M. Internet shutdowns in Africa threaten democracy and development. *The Conversation*. 26 July. Accessible at: https://theconversation.com/Internet-shutdowns-in-africa-threaten-democracy-and-development-142868; Internet Society. 2018. Policy Brief: Internet Shutdowns. 18 December. Accessible at: https://www.Internetsociety.org/policybriefs/Internet-shutdowns.

[21] UNHRC. 2013. Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/23/40, at para 60. Accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[22] *Ibid*.

[23] University of Minnesota. 1996. *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, U.N*. Doc. E/CN.4/1996/39. Minnesota: University of Minnesota. Accessible at: http://hrlibrary.umn.edu/instree/johannesburg.html.

CHAPTER 2 THE DIGITAL ECOSYSTEM

OBJECTIVES OF CHAPTER 2

In this chapter we will:

- Introduce the layer model of the Internet in order to frame a conceptual understanding of the digital ecosystem.
- Frame a conceptual understanding of what functions and relationships ICT policies typically govern.
- Identify which key role players are involved in the development of ICT policy and their respective and inter-related functions.

In Chapter 1 we discussed some of the imperatives underpinning the development of ICT policies worldwide. We showed how, through the development of effective ICT governance frameworks, ICTs can be leveraged to facilitate ambitious human development outcomes and good governance, as well as play a significant role in stimulating growth and accelerating socio-economic development. We also emphasised the importance of effectively coordinated, participatory and broadly representative ICT policy development initiatives. This is because, unlike with traditional telecommunications services which govern utilities within a single sector or national jurisdiction, ICT governance frameworks govern interactions and relationships within a complex digital ecosystem which spans multiple sectors and jurisdictions. This digital ecosystem is deeply inter-connected with, and inter-dependent on, global markets and systems of governance.

CASE STUDY: EU GDPR

The enactment of the European Union's General Data Protection Regulation 2016/679 of the European Parliament and the Council (EU GDPR) demonstrates the complexity and interconnectedness of the digital ecosystem particularly well. The GDPR provides for a set of rules for how the personal data of EU citizens may be collected, stored and transferred between the EU and non-EU jurisdictions, and the minimum legal standards and recommended protocols for protecting this data and the privacy of EU citizens online. Its impact is far reaching:

- *Because the EU represents a substantial market, businesses whose functioning relies on the collection and processing of user data such as Facebook were compelled to align those functions with GDPR in order to continue operating in or accessing European markets.*
- *Non-European governments whose agencies' operations depend on the collection and processing of European citizens' data are also compelled to renegotiate treaties and/or align their home countries' laws and regulations with GDPR in order to continue their operations in the EU. This was particularly impactful to the operations of surveillance and security agencies.*
- *At the time of writing, the European Court of Justice had recently handed down a ruling which prohibited the movement of user data from the EU to the USA by companies unless they could commit to safeguarding that data from being accessed by third parties including US intelligence agencies, failing which they would be violating users' right to privacy.[1] For technology companies*

[1] Hern, A. 2020a. Tech Firms Like Facebook Must Restrict Data Sent from EU to US, Court Rules. The Guardian. 16 July. Accessible at: https://www.

> *like Facebook that process user data gathered from across the world, and exploit it to generate advertising revenue across and between jurisdictions, as well as for users and organisations which rely on the platforms they provide for their personal and commercial activities, this development posed substantial implications for how the operations of global technology companies based in USA, or whose businesses relied on the transfer of data between the EU and USA, were structured.*[2]

As can be seen from the EU GDPR study, the introduction of any new ICT governance frameworks can have substantial implications for more than just technology companies and their end-users in any one country. Political relations between both states and economic and political communities can also be impacted, as can be their economic relations and the effective functioning and growth of local industry's ability to participate in local and global markets. ICT governance frameworks, therefore, must be developed with a clear understanding of their direct and indirect implications for the digital ecosystems they operate within, and what this ultimately means for all role players within that ecosystem.

In order to develop this understanding, in this chapter, we will begin by unpacking the **structure** of the primary subject of ICT governance frameworks – the Internet itself – and the value-chain that enables it to operate as we enjoy it today. We will consider some of the main **role players** involved in developing ICT governance frameworks, and their respective roles and responsibilities. Lastly, we will consider the **relationships** that exist between the role players in each layer of this integrated value chain which necessitate a multi-layered approach to ICT governance.

2.1 The layer model of the Internet

Very simply, the Internet is a vast, global wide area network that connects computer networks and systems around the world with each other. Unlike traditional telecommunications like a phone or telefax whose functioning is premised on the availability of open and dedicated communication channels between users, the functioning of the Internet is premised on how the information that is communicated between users or systems is packaged and organised so as to enable transmission and reception regardless of whether the channel is open or closed.

This approach to structuring how communication between users and systems happens is what defines the Internet as a network of more or less autonomous networks held together by common principles and standards relating to how the information being communicated is handled. More than enabling users and systems which are directly connected to one another, the Internet enables them to connect and communicate with users and systems across networks provided that they mutually conform with these minimum principles and standards at four levels or layers. And it is the collective functioning of each of these layers that makes up the Internet we enjoy today possible.

2.1.1 The physical layer

The Internet joins different packet-switching communications networks together, and is often described as a network for networks. At the physical layer, the Internet is made up of network nodes. These are physical devices like modems, switches, hubs, servers etc. which are able to send, receive or forward information to each other through a network connection. A network connection can be wireless – such as 3G or satellite – or a physical fixed line link between nodes – such as optical fibre cables.

theguardian.com/technology/2020/jul/16/tech-firms-like-facebook-must-restrict-data-sent-from-eu-to-us-court-rules.

[2] Manancourt, V. 2020. Top Facebook exec pushes back on talk of Europe withdrawal. Politico. 23 September. Accessible at: https://www.politico.eu/article/nick-clegg-top-facebook-executive-pushes-back-on-talk-of-europe-withdrawal/; Hern, A. 2020b. Facebook Says It May Quit Europe Over Ban on Sharing Data with US. The Guardian. 22 September. Accessible at: https://www.theguardian.com/technology/2020/sep/22/facebook-says-it-may-quit-europe-over-ban-on-sharing-data-with-us.

The physical layer is controlled by the different network operators and Internet service providers in order to provide users with access to the Internet. This is usually a state-owned telecommunication company, although there may also be one or several privately owned network providers and Internet service providers (ISPs).

Even though these network operators and ISPs are often competitors, they are usually aligned in their interests. This is because they all rely on the state to use and/or gain access to network infrastructure and/or frequency spectrum which enables fixed line and wireless telecommunication services, as well as on each other to be able to exchange access to each other's networks.

Some of the most significant ICT governance issues which arise from the physical layer of the Internet include:

- **Establishing frameworks for who can rollout network infrastructure in what areas.** This includes minimum norms and standards for the quality and speed of network services.
- **Pricing and affordability issues related to access and use of network services.** These are usually linked to ownership and control dynamics in what is usually a highly concentrated or monopoly-controlled market.
- **Determining the kind of information that can be transmitted between network nodes and under what conditions this may happen.** This is most of often seen at the level of debates about what kind of content coming from which network nodes may be prioritised, filtered or blocked (network neutrality, content filters and intentional network disruptions), as well as who should ultimately bear responsibility for the content that is transmitted over a network (intermediary liability).

2.1.2 The code layer (or the "protocol stack")

This layer, also known as the "protocol stack", pertains to the technical standards designed to enable communications across a network. It not only defines how different nodes and elements on the Internet are able to identify each other in order to communicate, but also the protocols or procedures by which they can transmit information between each other in the communication. The different protocols in the protocol stack each enable different aspects of communication across the Internet, and work together to enable the Internet to run on almost any type of physical infrastructure, and carry any type of information.

The management of the operation and databases related to how all the network nodes and elements are able to identify one another – Internet protocol (IP) addresses and domain name systems – are managed and overseen by a non-profit organisation based in the USA called the Internet Corporation for Assigned Names and Numbers (ICANN). The technical standards and communication protocols which define how the information that is communicated between nodes and elements is processed and transmitted are overseen by an association of experts called the Internet Engineering Task Force (IETF).

Some of the most significant ICT governance issues that arise from this layer of the Internet include:

- **Rules and procedures pertaining to how domains are assigned and operated, and by whom.** Whereas ICANN oversees the databases related to the name spaces and numerical spaces, as well as the root name servers that operate the domain name systems (DNS), the registries for top-level domains such as *.org; .africa;* .co etc. are delegated to registrars to sell as domain names such as .
- **The protocols by which networks may manage their own operations.** This includes developing more efficient ways to run autonomously as they become larger and more complex.
- **The protocols by which physical objects and devices connected in a network may communicate with one another, their operators and their manufacturers.** This in order to provide continuous

network functions and services. This is called "the Internet of things", and has significant implications for issues such as surveillance, data sovereignty and privacy amongst others.

2.1.3 The application layer

The application layer is made up of software that allows users to interact over the Internet. It includes, for instance, applications from browsers, search engines, social networking platforms, email clients and software that enables voice and text messaging services to operate over the Internet rather than over traditional telecommunication channels like fixed-line and wireless networks.

Unlike the other layers of the Internet which are overseen or managed by certain bodies, anyone can create any application they choose to the extent that this code conforms with the established minimum technical standards and protocols which enable network communication over the Internet. Because of its openness, the scope for innovation on this layer of the Internet is almost boundless. It has enabled the development of software that has revolutionised how people can communicate and complete tasks with maximum efficiency, as well as enabling the emergence of powerful technology companies such as Google, Facebook and Yahoo!.

Some of the most significant ICT governance issues that arise from this layer of the Internet include:

- **Setting standards and procedures for assuring the security and quality of applications.** This usually happens directly between the user and application provider through terms of use agreements. However, this relationship can also occur between application manufacturers and intermediaries who deliver those applications to market, such as Apple and Google's respective app stores or Firefox's plug-in store, which set minimum security and quality standards which developers of applications hosted on their platforms must comply with.

- **Setting standards and procedures for assuring the privacy of user data and communications collected and processed by these applications from surveillance.** In recent years, this issue has expressed itself in the form of the push for end-to-end encryption for communications applications such as WhatsApp, Skype and Signal in order to mitigate state surveillance of communications. This consideration is also what underpinned the set of issues leading to the development and enactment of the EU's GDPR.

- **Creating the conditions for competition access and choice for users of these applications.** Because they are the tools by which users are able to perform tasks, software applications play a crucial role in the digital ecosystem. As a result, the efficiency by which these applications are able to perform these tasks easily, accurately and securely becomes their competitive advantage. It is often commercialised, and forms the basis for the emergence of powerful technology companies like Google and Facebook who either provide their applications and services to users at a cost or lock users into a relationship of dependency on them. Although software developers have a right to benefit from their innovation and investment in developing these applications, the negative consequences that can flow out of these dynamics are many:

  » Users who cannot afford user licenses can be locked out of meaningful participation in environments which require knowledge and use of these applications, thereby entrenching the digital divide.

  » Widely used applications with no alternatives can be subjected to state surveillance practices. Where these applications enjoy market dominance or monopolies, users are unable to opt-out or find suitable alternatives. This can increase their exposure to violations of their privacy.

  » As reliance becomes concentrated around one or a small handful of commercial applications or their providers, the resilience of the networked communities around them is negatively impacted when problems arise with the application impacting directly on all of their users. An example of this is if a Facebook/WhatsApp or Instagram server fails or is interrupted, many or all users who depend on Facebook/WhatsApp or Instagram to communicate or do business may be unable to do so until it is resolved.

The open source and free software movement has, for decades, been at the forefront of developing and promoting applications which can form open, secure and reliable alternatives to users. This has produced tools applications like the Firefox web browser; OpenOffice and LibreOffice suites; The Tor suite of products which enables anonymous and encrypted browsing and communication, as well as initiatives such as the Mozilla Foundation[3] and Open Technology Fund[4] which support and facilitate the development of open access technologies.

2.1.4 The content layer

This layer consists of the information that the Internet's users share, publicly and privately, across the network. It includes, for instance, emails, photographs, videos and music. All users shape the content layer through the information shared online.

This layer is closely connected to the application layer, and it is usually the case that decisions concerning the functioning of the application layer have direct implications for the kind of content we are able to share and under what circumstances. Indeed, this is often where the most significant debates around the rights and responsibilities of all role players in the digital ecosystem are most robustly contested.

Some of the most significant ICT governance issues that arise from this layer of the Internet include:

- **Regulating what content may be transmitted between users on the Internet and under what circumstances.** This can range from prohibitions on the possession and publication of child sexual exploitation content to developing frameworks for regulating speech acts by online news and information services and citizens.

- **Managing copyright regimes and enforcing claims.** Because so much commercial and non-commercial content is available to and is being exchanged by users of the Internet, new challenges concerning how copyright should best be structured and enforced online emerge. These debates have produced applications such as digital rights management tools which aim to control the redistribution of digital media at the application layer of the Internet, as well as new kinds of copyright regimes such as the Creative Commons License[5] which enable rights' holders to be able to enjoy many of the benefits that flow from their innovation while still enabling others to freely distribute, use or build upon their work.

- **Defining who should ultimately be responsible for regulating, monitoring and enforcing laws concerning prohibited speech acts online.** In some jurisdictions, the law may place that burden on intermediaries such as application developers or even ISPs, while in other jurisdictions, this is directly the responsibility of the state.

2.2 Disparate but connected

To sum up briefly, the Internet can be understood as the collective functioning of each of these layers. Although each of these layers is distinct from each another, with their disparate sets of considerations and issues concerning their functioning and governance, they are deeply connected to one another, with all

[3] Mozilla Foundation. Accessible at: https://www.mozilla.org/en-US/moss/.

[4] Open Technology Fund. Accessible at: https://www.opentech.fund.

[5] Creative Commons License. Accessible at: https://creativecommons.org.

role players at each level having a stake in the outcomes of the decisions made at each level. Therefore, if any one of these layers is not functioning optimally, the Internet as a whole cannot operate optimally.

This inter-connectedness and inter-dependence is not limited to the technical functioning of the Internet alone, but has substantial social, economic and political implications too. For example, laws which make intermediaries liable for the content that is transmitted on their applications and networks can very easily be invoked by the state to co-opt platforms like Facebook or ISPs to spy on and censor the communications of users at a mass scale.

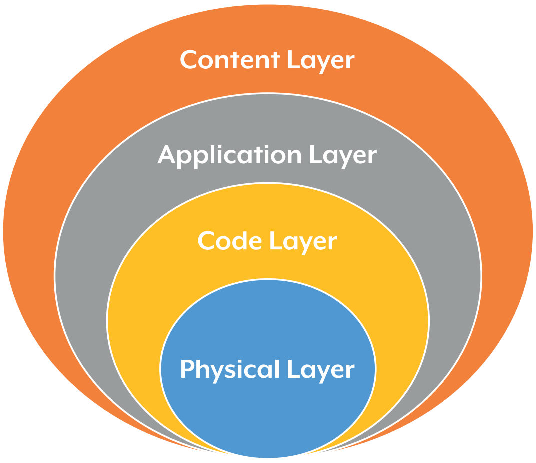

Illustration 2: Graphic representation of the layer model of the Internet
Source: Sekoetlane Phamodi (author), 2020; based on Global Partners Digital, 2014 (pp28-42)

ICT policies may address one or more of the abovementioned layers, depending on the nature and scope of the policy in question. For example, an ICT policy geared towards broadband infrastructure will be more targeted towards the physical layer, whereas a policy that imposes restrictions on online content will be more targeted towards the content layer. Other policies may deal directly with multiple layers, such as a cybersecurity policy that deals with both infrastructure and content.

2.3 Relationships produced by the layer model of the Internet

From Illustration 2 above, the role players who have a stake in the decisions of each layer are not necessarily confined to those layers. Especially in contexts where there is increasing vertical integration between the functions of each layer, the people responsible for providing network infrastructure can be the same people deciding on which applications enjoy priority treatment on those networks, as well as what kind of content is ultimately available to end-users. Indeed, this is precisely what is at stake in the **net-neutrality** and **zero-rating** debates.

Ultimately, the various role players can and do operate across different layers to the extent that the decisions taken about those layers impact on their interests. In some layers, role players may find themselves aligned in their interests while, in others, those same role players may diverge completely. It is therefore important to consider the relationships and interplay between these role players across all levels when considering how to approach responding to ICT governance problems. Six symbolic kinds of relationships exist, as shown in Illustration 3 below:

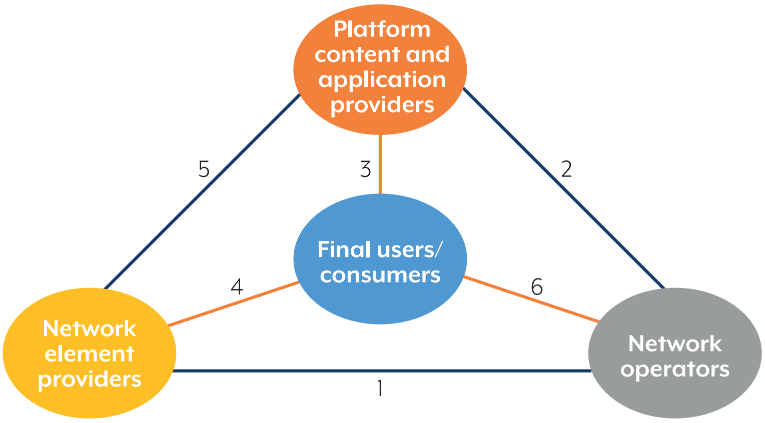
Platform content and application providers
5
3
2
Final users/ consumers
4
6
Network element providers
Network operators
1

Illustration 3: Graphic representation of the symbolic relationships between stakeholders at different layers of Internet
Source: Sekoetlane Phamodi (author), 2020

- **Relationship 1: Between network element providers and network operators.** Network operators purchase network elements from network element providers, such as switches, routers or systems software. These two categories of role players mutually depend on and cooperate closely with one another.
- **Relationship 2: Between network operators and platform content and application providers.** In this relationship, network operators provide inputs that are used by the content and application providers to produce outputs. An example of this is in how an application like WhatsApp or Skype relies on the fixed line or wireless networking service provided by a telecommunications operator such as Safaricom to deliver its over-the-top voice, text-based and video calling services.
- **Relationship 3: Between content and applications providers and final consumers.** This relationship concerns how application and content services interact with their users to facilitate the production and delivery of content/communications to them. Issues emerging from this relationship include the security of the applications for their purpose in the case of electronic commerce platforms, or the credibility of the content offered in the case of news and information services. It can also extend to the community standards which regulate the behaviour of users on applications which deliver user-generated content like Facebook or YouTube.
- **Relationship 4: Between network element providers and final users/consumers.** This relationship is similar to Relationship 1. Here, consumers rely on network element providers for the physical infrastructure they need to be able to access the Internet. This can be in the form of personal computers or smartphones, servers and modems. Sometimes network element providers and network operators are one and the same. This can have implications on issues like the interoperability of network elements between networks operated by different operators.
- **Relationship 5: Between network element providers and platform content and application providers.** This relationship is similar to Relationship 2. For example, content and application providers such as Facebook rely on network element providers such as Apple to be able to deliver their mobile apps to iOS users. As with relationship 2, the network element providers provide a production and innovation platform for the platform content and application providers. They also set the rules and standards which content and application providers must adhere to in order to continue operating on their platforms.
- **Relationship 6: Between network operators and final consumers.** This includes the provision of fixed voice, mobile and Internet access services to customers.

Each of the abovementioned relationships operates within its particular context and is influenced by the dynamics within that context. For example, the cost at which final users are able to access network services in a context with a single state-owned network operator will not be the same as in a context with several public- and privately-owned network operators.

In developing ICT governance frameworks which intend to respond to the tensions between, as well as risks and opportunities brought about by these relationships, policy makers therefore have to pay attention to and consider all the factors which influence those relationships. These can include the following:

- **Policy frameworks**. This factor relates to the prevailing policies, legislation and regulations governing the relationships and interactions between the various role players. This can include everything from the rules and regulations governing how network infrastructure is rolled out through to legislation defining the limitations on permitted speech acts such as hate speech or defamation laws.

- **Institutional arrangements**. This factor relates to the formal institutions that are responsible for overseeing the performance of role players in their mutual and respective functions, as well as facilitating the healthy functioning of the ecosystem in line with the stated policy aspirations. This can include universal service funds which facilitate the rollout of network services in order to widen coverage and reach, and regulatory authorities which assure and enforce the quality of services offered by role players.

- **Market dynamics and competition**. This factor concerns both the demand- and supply-side conditions which enable fair and equitable entry and participation in the ecosystem. It relates to issues like how ownership and control of network infrastructure and operators may be structured, as well as the pricing and affordability of the services they offer.

- **User and industry formations**. This factor relates to the relationships and alliances that emerge among and between the role players themselves, and how these are mobilised to advance their interests. Content and application providers can form industry associations through which they negotiate and lobby for certain policy outcomes that affect the sector as a whole. For example, consumer protection groups may organise to demand action which protects them from unfair pricing behaviours by network operators, or violations of their rights by content and application providers.

Because of its nature as a network of networks with no central authority, governance of the Internet happens at different levels and through mutual cooperation between stakeholders. For instance, the high-level rules governing how frequency spectrum (that makes wireless networking possible) is used are determined at a global level by a UN body called the International Telecommunication Union (ITU); but how usage of that frequency spectrum is assigned and managed is determined at state level by national governments. Similarly, the rights and responsibilities all stakeholders have towards one another, though guided by public international law and principles defined through treaties and trade agreements, are only enforceable to the extent that national governments have jurisdiction over those role players.

This set of arrangements therefore requires that policy makers are aware of, but preferably engaged with, the processes, relationships and interactions between the various bodies which inform and make the top level decisions relating to how the Internet operates. These bodies may include:

- **National governments**. They decide, through their own political processes, how the digital ecosystem under their jurisdiction will be governed to produce the social, economic and political outcomes that suit their contexts.

- **Global and regional governance bodies and fora**. These include ICANN, the ITU, and regional and global Internet governance fora (IGFs). Treaty bodies and regional mechanisms such as the Economic Community of West African States (ECOWAS) and the African Commission on Human and Peoples' Rights (ACHPR) may also set binding rules, standards and frameworks for how members of the communities they preside over should approach Internet governance under their collective and respective jurisdictions.

- **Multilateral agencies**. These include the World Bank or the New Partnership for Africa's Development (NEPAD) and international donor agencies. They may be able to influence ICT policy outcomes through the support they offer at state or regional level. For example, they may offer or withhold financial or technical support on the condition that national governments take steps or decisions which produce certain policy outcomes within or through the digital ecosystem such as open governance, liberalised markets, and deepened freedom of information and expression.

- **Global actors and associations**. These include Google, Facebook or Groupe Spéciale Mobile Association (GSMA). They represent individual actors with international footprints or multiple actors across the world with shared interests. Because of their global market dominance and/or their representative power, they enjoy significant influence over decisions impacting on their respective operations and mutual interests at a global level.

Ultimately, the digital ecosystem must be understood as a multi-layered and multi-stakeholder environment in which different actors with both different and shared interests and levels of influence co-exist and interact to produce the outcomes that best suit them and the myriad communities of users of the Internet. Illustration 4 below illustrates this multi-layered model of the digital ecosystem and the relationships between its different elements, as well as the kinds of outcomes that are produced from their interactions.

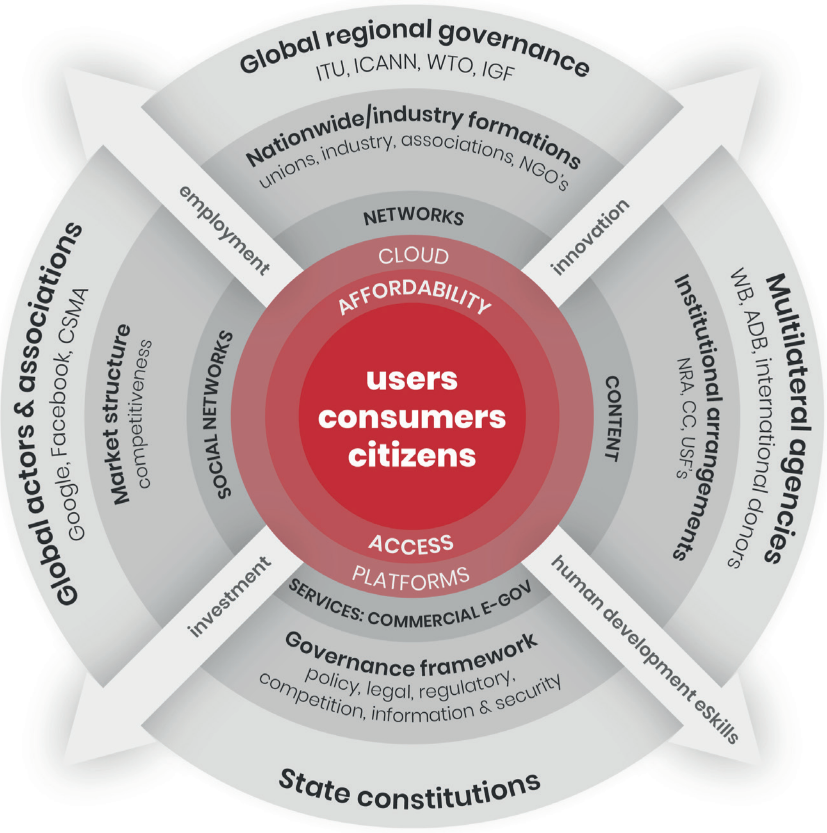
Global regional governance
ITU, ICANN, WTO, IGF
Nationwide/industry formations
unions, industry, associations, NGO's
NETWORKS
CLOUD
AFFORDABILITY
users
consumers
citizens
ACCESS
PLATFORMS
SERVICES: COMMERCIAL E-GOV
Governance framework
policy, legal, regulatory,
competition, information & security
State constitutions
Global actors & associations
Google, Facebook, CSMA
Market structure
competitiveness
SOCIAL NETWORKS
CONTENT
Institutional arrangements
NRA, CC, USF's
Multilateral agencies
WB, ADB, international donors
employment
innovation
investment
human development eSkills

Illustration 4: Multi-layered governance of digital ecosystem
Source: NPC, 2020[6]

[6] National Planning Commission, Republic of South Africa. 2020. Draft Digital Futures South Africa's Digital Readiness for the Fourth Industrial Revolution. Accessible at: https://www.tralac.org/documents/resources/by-country/south-africa/3902-draft-digital-futures-south-africas-digital-readiness-for-the-fourth-industrial-revolution-npc-july-2020/file.html.

CHAPTER 3 RIGHTS AFFECTED BY ICT POLICY MAKING

OBJECTIVES OF CHAPTER 3

In this chapter we will:

- Frame which rights are most directly impacted by information and communication technology (ICT) policies and how.
- Consider the public international law implications for how ICT governance frameworks are developed.
- Reflect on some of the most significant legal challenges and debates concerning human rights and the Internet.
- Consider some existing principles and instruments for how domestic and public international law has been applied to selected ICT governance and human rights problems in Africa.

As we explained in Chapter 2, by design, the Internet's architecture is underpinned by end-to-end communication between users across a decentralised global network of networks. What this means is that, in principle, for the Internet to be able to function in the way that we enjoy it today, anyone anywhere in the world should be able to share information and ideas from any point in the global network of networks to another without having to ask any one authority for permission to do so.

In essence, the Internet can be said to be designed in such a way that it provides the means for the fullest expression of the right to **freedom of expression** as defined in public international law instruments including, most significantly, the **Universal Declaration of Human Rights** (UDHR) which, in **Article 19**, states that:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

As a consequence of this design, the unique characteristics of the Internet enable it to play a key role in facilitating the expansion of how we might understand and enjoy a range of other rights.

In this chapter we will discuss the intersection of human rights with technology, particularly in respect of the Internet, as well as some of the most significant issues and debates emerging at the intersection. We will discuss the rights to freedom of expression, information and privacy as the rights most directly impacted through ICT policy making with reference to the guidance public international law provides on how to approach them.

3.1 Situating human rights on the Internet

Through their use of the Internet, people and organisations are empowered to continuously develop new technologies and facilities which rely on connectivity to this global network of networks to enable users in order to, for example, access information and impart ideas, associate and assemble online, as well as access knowledge and produce cultural content. All the time people are developing and using tools like e-mail or over-the-top (OTT) multimedia communication tools like WhatsApp, WeChat and Signal to talk and share content with one another about significant political issues as well as connecting with colleagues and loved ones. Social networks and bulletin boards like Facebook groups, Reddit channels and online forums are being used to build communities around topics of mutual interest, becoming as much the site of association and assembly as the means by which people communicate with one another. Platforms like Wikipedia and YouTube are also developing into information and cultural commons, functioning as knowledge repositories as well as teaching and learning tools which make knowledge and cultural exchange all the more possible regardless of the frontiers of time, space, language or belief.

By the same measure, we are also witnessing how activities conducted by individuals or groups online can have very direct "real world" consequences. We have seen how, through the amplification power of social networks, for example, harmful speech acts or disinformation can spread very quickly and pose substantial reputational damage, as well as serious human security risks.[1] For women, in particular, we have seen how targeted online harassment can amplify their lack of personal safety, as well as deepen emotional and psychological distress.[2] These examples bring into focus the importance of establishing frameworks that can elaborate the rights and responsibilities people already enjoy in respect of their relationships with one another. And be applied in an increasingly technology mediated world.

At the same time, as much as technology enables us to expand how we understand and apply rights frameworks regardless of frontiers, it also calls us to rethink how these rights are balanced alongside others in line with the various public policy imperatives that are particular to, and demanding enforcement at, the state level. For example, as much as most countries might recognise the right to freedom of expression, they may have diverging public policy understandings pertaining to the scope of the enjoyment of that right and enforceable limitations on it which are particular to their context. This can present real challenges for governments in terms of reconciling their obligation to enforce public policy at national level with the open and decentralised nature of the Internet as a global network of networks. So how should these emerging public policy problems be approached?

Although there is no definitive answer to this question, there is universal agreement that a rights-based approach should be taken in navigating the new set of public policy problems brought about by the growing importance technology and the Internet, in particular, have in facilitating and mediating human relationships. A key point of departure, therefore, is the United Nation's (UN's) Human Rights Council's *Resolution 32/13* on the promotion, protection and enjoyment of human rights on the Internet[3] which affirmed two earlier resolutions[4] proclaiming that

> *The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights.*

[1] Wasserman, H. & Madrid-Morales, D. 2019. An Exploratory Study of "Fake News" and Media Trust in Kenya, Nigeria and South Africa. African Journalism Studies. 40:1, 107-123, DOI: 10.1080/23743670.2019.1627230; Kofi Annan Foundation. 2020. Protecting Electoral Integrity in the Digital Age: The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age. Accessible at: https://storage.googleapis.com/kofiannanfoundation.org/2020/05/85ef4e5d-kaf-kacedda-report_2020_english.pdf.

[2] Hinson, L., Mueller, J., O'Brien-Milne, L., Wandera, N. 2018. Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women. Accessible at: https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf; Iyer, N. et. al. 2020. Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet. Accessible at: https://www.apc.org/en/pubs/alternate-realities-alternate-Internets-african-feminist-research-feminist-Internet; https://www.mfwa.org/wp-content/uploads/2018/02/Baseline-Report-WRO-Issues-in-Ghana.pdf.

[3] UNESCO. 2016b.The Promotion, Protection and Enjoyment of Human Rights on the Internet. Montevideo: UNESCO. 32/13. Accessible at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Pages/ResDecStat.aspx.

[4] Ibid.

The resolution, which was adopted by consensus, frames an understanding of human rights on the Internet as requiring the same treatment as human rights offline, therefore demanding the consideration of the same norms, standards and legal principles in terms of how the enjoyment of those rights might be interpreted, limited or balanced against others. These norms, standards and legal principles include a responsibility on lawmakers and courts to consider issues such as the necessity of the limitation, its legitimacy, the proportionality of the limitation to the harm being prevented, as well as the fairness of the limitation so as to ensure the legal certainty under the rule of law, and the protection of citizens from undue encroachment on their rights in the name of a vague or unspecified purpose.

3.2 Freedom of expression and access to information

By now, freedom of expression is firmly entrenched in regional and international law frameworks, as well as in most domestic constitutions; and states are obliged to respect, protect and promote this right. In order to do so, states are required to take legislative and other measures in order to give effect to this right.

In essence, freedom of expression consists of three core elements:

- The right to hold opinions without interference (freedom of opinion).
- The right to seek and receive information (access to information).
- The right to impart information (freedom of expression).

In public international law, the right is derived in article 19 of the International Covenant on Civil and Political Rights (ICCPR) as follows:

> "(1) Everyone shall have the right to hold opinions without interference.
>
> (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

Similarly, the right is also entrenched in the African regional system, most notably in article 9 of the African Charter on Human and Peoples' Rights (the "African Charter"):

> "(1) Every individual shall have the right to receive information.
>
> (2) Every individual shall have the right to express and disseminate his opinions within the law."

The significance of this right as a facilitative right to the enjoyment of all other rights is well demonstrated in how it is expressly raised in a variety of regional instruments elaborating the highest aspirations for the rights of the people and relationships they govern. For example:

- Article 7 of the African Charter on the Rights and Welfare of the Child (ACRWC)[5] provides that every child who is capable of communicating their own views shall be assured the rights to express their opinions freely in all matters and to disseminate their opinions subject to such restrictions as are prescribed by laws. Article 9 provides further that every child shall have the right to freedom of thought, conscience and religion.

[5] AU. 1990. African Charter on the Rights and Welfare of the Child. Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-charter-rights-and-welfare-child.

- Article 27(8) of the African Charter on Democracy, Elections and Governance (ACDEG)[6] provides that, in order to advance political, economic and social governance, state parties must commit themselves to, among other things, "promoting freedom of expression, in particular freedom of the press and fostering a professional media".

- Article 6 of the Treaty for the Establishment of the East African Community[7] includes among its fundamental principles the principle of good governance, and states that this includes the principles of democracy, rule of law, accountability, transparency, and the rights contained in the African Charter. This has been applied by the East African Court of Justice (EACJ) to rule on matters regarding infringements of the right to freedom of expression.[8]

- Article 66 of the Revised Treaty of the Economic Community of West African States (ECOWAS) provides that members agree (i) to maintain within their borders, and between one another, freedom of access for professionals of the communication industry and for information sources; (ii) to facilitate exchange of information between their press organs; to promote and foster effective dissemination of information within ECOWAS; (iii) to ensure respect for the rights of journalists; and (iv) to take measures to encourage investment capital, both public and private, in the communication industries in member states.[9]

- Article 19(1) of the Southern African Development Community (SADC) Protocol on Culture, Information and Sport[10] provides that state parties will cooperate on improving the free flow of information within the region; and article 20 provides that state parties will take the necessary measures to ensure the development of media that are editorially independent and conscious of their obligations to the public and greater society.

The right to freedom of expression is further supplemented in the African Commission on Human and People's Rights (ACHPR's) Declaration of Principles on Freedom of Expression and Access to Information in Africa.[11]

The now revised Declaration provides substantive detail for how the right should be interpreted and enforced, including guidance for the application of the principles pertaining to technology and the Internet. More than extending the application of its interpretive framework for freedom of expression to the Internet, the Declaration now also places positive obligations on states to take the necessary steps to improve access to the Internet in order to facilitate maximum enjoyment of the right to freedom of expression.

However, rights are not absolute, and may be limited in appropriate circumstances when balanced against competing rights and interests.

[6] AU. 2007. African Charter on Democracy, Elections and Governance. Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-charter-democracy-elections-and-governance.

[7] EACJ. 1998. Treaty for the Establishment of the East African Community. Accessible at: https://www.eacj.org/?page_id=33#toc-article-6-fundamental-principles-of-the-community.

[8] See, for instance, EACJ. 2015. Burundi Journalists' Union v The Attorney General of the Republic of Burundi, Reference No. 7 of 2013. Accessible at: http://eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi.

[9] ECOWAS. 1975. Economic Community of West African States (ECOWAS) Revised Treaty. In UiO The Faculty of Law. Accessible at: https://www.jus.uio.no/english/services/library/treaties/09/9-01/ecowas_treaty_revised.xml.

[10] SADC. 2001. Protocol on Culture, Information and Sport 2001. Blantyre: SADC. Accessible at: https://www.sadc.int/documents-publications/show/797.

[11] ACHPR. 2019. Declaration of Principles on Freedom of Expression And Access To Information In Africa. Accessible at: https://www.achpr.org/legalinstruments/detail?id=69.

3.2.1 The limitation of rights

Both the ICCPR and the African Charter set out the grounds on which the right to freedom of expression may be limited:

- In respect of the ICCPR: Article 19(3) provides that the right to freedom of expression may be limited on the basis of respect of the rights and reputations of others; the protection of national security or public order; the protection of public health; or the protection of morals. Article 20 provides further to identify those categories of speech that must be prohibited by law: any propaganda for war; or any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
- In respect of the African Charter: Article 9(2) contains an internal limitation that every person has the right to freedom of expression "within the law".

In **Media Rights Agenda and Constitutional Rights Project v Nigeria,12** the ACHPR (at para 66) interpreted this as meaning "within international law", explaining that to do otherwise would "defeat the purpose of the rights and freedoms enshrined in the Charter" and that "international human rights standards must always prevail over contrary national law". In terms of the grounds on which the right to freedom of expression may be limited, the general limitations clause in article 27 of the African Charter makes reference to the rights of others; collective security; morality; or common interest.

A three-part test is used to determine whether the limitation is justifiable:

- The limitation must be provided in law.
- It must pursue a legitimate aim.
- It must be necessary for a legitimate purpose.

As explained in the UN Human Rights Committee's General Comment No. 34 on article 19 of the ICCPR (at para 21), restrictions on the right must not put the right itself in jeopardy. Furthermore, in respect of the requirement of proportionality, General Comment No. 34 explains (at para 34) that: (i) restrictive measures must be appropriate to achieve their protective function; (ii) they must be proportionate to the interest to be protected; (iii) the principle of proportionality must be respected both in law and by the authorities applying the law; and (iv) the principle of proportionality must take into account the form of expression and the means of dissemination, for instance if it pertains to a public debate concerning figures in the public and political domain.

[12] ACHPR. 1998. Media Rights Agenda, Constitutional Rights Project, Media Rights Agenda and Constitutional Rights Project v Nigeria. Accessible at: http://www.worldcourts.com/achpr/eng/decisions/1998.10.31_Media_Rights_Agenda_v_Nigeria.htm.

ZIMBABWE LAWYERS FOR HUMAN RIGHTS AND ANOTHER / REPUBLIC OF ZIMBABWE

Source: ACHPR Communication No. 284/03, https://www.achpr.org/public/Document/file/English/achpreo6_284_03_eng.pdf

The applicants in the matter challenged the Access to Information and Protection of Privacy Act, 2002 before the ACHPR, arguing that the effect of the legislation prohibited mass media services from operating until they have registered with the Media and Information Commission. The second applicant, Associated Newspapers of Zimbabwe (ANZ), challenged the constitutionality of the registration requirement, and declined to register until the question of the constitutionality had been determined by the Supreme Court.

However, the Supreme Court stated in its ruling that: "The applicant is operating outside the law and this Court will only hear the applicant on the merits once the applicant has submitted itself to the law". Following the decision of the Supreme Court, 'The Daily News' was forcibly closed, the assets of ANZ were seized, and ANZ officials were arrested or threatened.

Before the ACHPR the applicants argued that this was, amongst other things, a limitation of the right to freedom of expression under article 9 of the African Charter. In determining whether the limitation of the right was justifiable, the ACHPR explained (at paras 175-176) as follows:

"It is alleged that the State moved into action to seize the premises and close the offices of the Complainants after the Court's decision.

Can it be said that the State was enforcing a Court decision or trying to prevent a breach of the law? The African Commission is of the view that even if the State was in the process of ensuring respect for the rule of law, it ought to have responded proportionally. In law, the principle of proportionality or proportional justice is used to describe the idea that the punishment of a certain crime should be in proportion to the severity of the crime itself. The principle of proportionality seeks to determine whether, by the action of the State, a fair balance has been struck between the protection of the rights and freedoms of the individual and the interests of the society as a whole. In determining whether an action is proportionate, the Commission will have to answer the following questions:

- *Were there sufficient reasons supporting the action?*
- *Was there a less restrictive alternative?*
- *Was the decision making process procedurally fair?*
- *Were there any safeguards against abuse?*
- *Does the action destroy the very essence of the Charter rights in issue?*

The ACHPR concluded (at para 179) that the action taken by the respondent state to stop the applicants from publishing their newspaper, close their business and seize their equipment resulted in them and their employees not being able to express themselves through their regular medium, and to disseminate information; and that this was a violation of the right to freedom of expression under article 9 of the African Charter. Furthermore, it held that the confiscation of their equipment and depriving them of a source of income and livelihood was a violation of the right to property under article 14 of the African Charter; and that by closing their business premises and preventing them from being able to work, this was a violation of their right to work under article 15 of the African Charter.

Principle 9 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa[13] sets out a scheme not dissimilar to the ICCPR's on how these rights may be justifiably limited. Significantly, it requires compliance with the following principles as regards the enactment of any laws or proclamations which may have the effect of limiting freedom of expression and access to information:

- The law must be clear, precise, accessible and foreseeable.
- The law must be overseen by an independent body in a manner that is not arbitrary or discriminatory.
- The law must effectively safeguard against abuse, including through the provision of a right of appeal to independent and impartial courts.

Further, the ACHPR now provides guidance on how to determine necessity and proportionality in laws which may have the effect of limiting the enjoyment of these rights. The law must:

1. Originate from a pressing and substantial need that is relevant and sufficient.
2. Have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim.
3. Be such that the benefit of protecting the stated interest outweighs the harm to the expression and disclosure of information, including with respect to the sanctions authorised.

So what guidance does this provide for the enjoyment of freedom of expression and access to information online?

3.2.2 Media and content regulation

As already noted, article 19(2) of the ICCPR makes clear that the right to freedom of expression applies "regardless of frontiers", and that the medium through which the speech is communicated does not affect the ambit of the protection that the right conveys. This includes Internet-based modes of communication.

In General Comment No. 34 on article 19 of the ICCPR, the UN Human Rights Committee made clear (at para 15) that states must take all necessary steps to foster the independence of new forms of media that have arisen through ICTs, and further (at para 39) that states must take into account both the differences and points of convergence in print and broadcast media on the one hand, and the Internet on the other.

Historically, different forms of media were regulated differently; for instance, print media was typically self-regulated, while broadcast media often had more involvement from the state. The significance of this distinction, however, has diminished considerably over time.[14] There is ever-increasing convergence between the traditional and digital media sectors, including in respect of infrastructure that is increasingly becoming inter-dependent. The recognition by the UN Human Rights Council and by the ACHPR that the right to freedom of expression must be equally protected both offline and online is therefore appropriate, and pays due regard to the convergence of different mediums and platforms through which the right to freedom of expression is exercised.

Types of content restrictions may include defamation laws, prohibitions on hate speech, and measures taken against copyright infringements. While the purported aim of the restriction may be, for instance, to limit the spread of disinformation or to address harmful speech online, in reality content restrictions have

[13] ACHPR. 2002. Declaration of Principles on Freedom of Expression in Africa, 32nd Session In University of Minnesota, Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia. Minnesota: University of Minnesota. Accessible at: http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html.

[14] Salmon, E. 2016. 'Independent regulation of broadcasting: A review of international policies and experiences'. Montevideo: UNESCO. Accessible at: http://unesdoc.unesco.org/images/0024/002460/246055E.pdf; Fielden, L. 2012. Press regulation: Taking account of media convergence', Foundation for Law, Justice and Society. England: University of Oxford. Accessible at: http://www.fljs.org/sites/www.fljs.org/files/publications/Fielden.pdf.

also been used by states to quell criticism and dissent, which is an unjustifiable limitation of the right to free speech.

3.2.3 Interference with network services and infrastructure, including Internet shutdowns

Network carriers, Internet service providers (ISPs) and platforms can also restrict content in several ways. This might be done in terms of their own internal policies, or in terms of a law or instruction by the state. This includes measures aimed at blocking and filtering content, which can hinder the full enjoyment of the right to freedom of expression. The terms "blocking" and "filtering" in this context are explained as follows:[15]

> *The difference between "filtering" and "blocking" is a matter of scale and perspective.*
>
> - *Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;*
> - *Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist.*

In both instances, the effect is that the platform and the content it delivers cannot be accessed, thereby limiting the ability of users to fully exercise their rights to information and expression. While there may be legitimate cause for states to require that network carriers, ISPs and platforms employ these practices for the purposes of enforcing public policy imperatives such as preventing the publication and distribution of child sexual abuse content or hate speech, states must apply the three-part test and enforce the public policy imperatives in a manner that is least restrictive to the enjoyment of the right to freedom of expression.

An Internet shutdown (commonly referred to as a 'kill switch'), however, is a drastic measure that entails the intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[16] This can be at the bidding of the government with the assistance of a private sector actor, and is typically intended to control or curb what people say or do.[17] Shutdowns may affect towns or regions within a country, an entire country, or even multiple countries, and have been seen to range from several hours to several months.[18]

Internet shutdowns have frequently been seen to take place without an empowering legal provision. For instance, in *CM Pak Limited v Pakistan Telecommunication Authority*,[19] the Islamabad High Court in Pakistan ruled that the Federal Government and the Pakistan Telecommunication Authority had impermissibly suspended or caused the suspension of mobile cellular services or operations in Pakistan. In terms of the domestic law, mobile services or operations could only be suspended if the President proclaimed a state of emergency. In the absence of any such proclamations – and notwithstanding national security concerns – any actions, orders or directives issued by the Federal Government or the Telecommunication Authority was illegal, *ultra vires* and without lawful authority and jurisdiction.

However, even in circumstances where the network disruption is ordered in terms of an empowering legal provision, these measures will still arguably fail to meet the standard of necessity and proportionality.[20]

[15] ARTICLE 19. 2016. Freedom Of Expression Unfiltered: How Blocking And Filtering Affect Free Speech. (London: ARTICLE 19), 7. Accessible at: https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf.

[16] Access Now. *What is an Internet shutdown?* Accessible at: https://www.accessnow.org/keepiton/?ignorelocale.

[17] *Ibid*.

[18] *Ibid*.

[19] Sebastian, M. Pak Court Holds Suspension Of Mobile Services By Federal Govt On Ground Of National Security Illegal. *Live Law*. Accessible at: http://www.livelaw.in/pak-court-holds-suspension-mobile-services-federal-govt-ground-national-security-illegal-read-judgment/.

[20] OHCHR. 2017. *Report of the UN Special Rapporteur on Freedom of Expression to the UN General Assembly, A/HRC/35/22*. Accessible at: http://

At present, there are currently court cases pending in Uganda and Cameroon that seek to challenge the constitutionality of the Internet shutdowns that occurred in these countries.[21]

In 2016, the UN Human Rights Council stated that it "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures".[22] Later that year, in November 2016, the ACHPR adopted Resolution 362(LIX) 2016, in which it expressed concern at "the emerging practice of State Parties of interrupting or limiting access to telecommunication services such as the Internet, social media and messaging services, increasingly during elections".

Since then, Principle 38(2) of the Declaration of Principles now unequivocally prohibits states from engaging or condoning any disruption of access to the Internet and other digital technologies for segments of the public or an entire population, putting to rest the question of whether African states may legitimately resort to this measure under any circumstances.

3.2.4 Intermediary liability

Internet intermediaries – the entities that provide services that enable people to use the Internet – are key role players in ensuring that the Internet is made available and accessible to users. Internet intermediaries fall into two categories: (i) conduits: technical providers of Internet access or transmission services; and (ii) hosts: providers of content services such as online platforms (e.g. websites), caching service providers and storage services.[23] More simply, Internet intermediaries can be described as the pipes through which Internet content is transmitted and the storage spaces in which it is stored. They are essential to the functioning of the Internet.[24] This includes network operators, network infrastructure providers, ISPs, hosting providers, social networks, and search engines.[25]

The imposition of intermediary liability, particularly where this is state-led, can result in undue burdens being placed on Internet intermediaries, and have a chilling effect on right to freedom of expression as it is a different form of content restriction. This includes, for example, circumstances where a government seeks to hold an ISP or website liable for content created by users of those services.[26] Within the context of the state's duty to protect, a report by UNESCO identified the following key aspects regarding intermediary liability:[27]

"1. The characteristics of intermediary liability regimes or lack thereof, as well as the regulatory objectives of the regimes (as elaborated in Chapter 2) affect intermediaries' ability to respect freedom of expression. Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of Internet services that facilitate expression.

2. Laws, policies, and regulations requiring intermediaries to carry out content restriction, blocking, and filtering in many jurisdictions are not sufficiently compatible with international human rights standards for freedom of expression.

ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22/Add.4.

[21] Dahir, A.L. 2018. Cameroon Is Being Sued for Blocking The Internet in its Anglophone Regions. *Quartz Africa*. Accessible at: https://qz.com/africa/1192401/access-now-and-Internet-sans-frontieres-suecameroon-for-shutting-down-the-Internet/; Unwanted Witness. 2017. *Court Adjourns Social Media Shutdown Lawsuit*. Accessible at: https://unwantedwitness.or.ug/court-adjourns-social-media-shutdown-lawsuit/.

[22] ACHPR. 2016. *362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016*. Banjul: ACHPR. Accessible at: https://www.achpr.org/sessions/resolutions?id=374.

[23] Association for Progressive Communications. 2014. *Frequently asked questions on Internet intermediary liability*. Accessible at: https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-Internet-intermed.

[24] Comninos, A. 2012. *The liability of Internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain.* Johannesburg: APC, 5.

[25] *Op. cit.*, 4.

[26] *Op. cit.*, 6.

[27] UNESCO. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries.* Montevideo: UNESCO, 179-180. Accessible at: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

3. Laws, policies, and practices related to government surveillance and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequately protect users' privacy.

4. Licensing agreements can affect intermediaries' ability to respect freedom of expression. This applies to ISPs in all countries studied and social networks and search engines in some countries.

5. Whereas due process generally requires that legal enforcement and decision making are transparent and publicly accessible, governments are frequently opaque about requests to companies for content restriction, the handover of user data, and other surveillance requirements. This makes it difficult for the public to hold governments and companies appropriately accountable when users' right to freedom of expression is unduly restricted – either directly, or indirectly through the compromise of user privacy."

Users rely on Internet intermediaries to exercise their rights online, and the right to freedom of expression requires intermediaries to be appropriately protected from liability for content generated by others.

REGULATORY MODELS OF INTERMEDIARY LIABILITY

Source: ARTICLE 19, Internet intermediaries: Dilemma of liability', 2013b, p 6, accessible at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

The three models of intermediary liability have been summarised as follows:

- **Strict liability model**. *Internet intermediaries are liable for third-party content, and intermediaries are effectively required to monitor content in order to comply with the law. This is used, for example, in China and Thailand.*
- **Safe harbour model**. *This grants intermediaries immunity, provided that they comply with certain requirements. This includes, for example, the notice and take-down procedure. This is used, for example, in France and the United Kingdom.*
- **Broad immunity model**. *This grants Internet intermediaries broad or conditional immunity from third party content, and exempts them from any general requirement to monitor content. This is used, for example, in Singapore and the EU.*

As a note of caution, it must be considered that any regulatory approach that imposes a form of intermediary liability has the potential to cause infringements to the right of freedom of expression, particularly if the intermediary errs by removing lawful content. Practically, the consequent effect of intermediary liability is that it gives intermediaries quasi-judicial authority to decide about the legality of content in circumstances where they may be ill-equipped to do so, and are not required to follow due process procedures, make their decisions transparent or offer independent appeals mechanisms.[28]

At the same time, it cannot be ignored that impermissible content, such as incitement to violence, is shared on platforms in circumstances where the individuals responsible for publishing the content cannot be identified. A useful safeguard that lawmakers should consider is for content restrictions to only be imposed on an intermediary when done in terms of a lawful order of court. This seeks to strike the appropriate balance between the relevant rights, including the right to freedom of expression, while addressing the reality that circumstances may arise in which content should properly be removed from online platforms.

[28] ARTICLE 19. 2013a. *Freedom of Expression and ICTs: Overview of International Standards*. London: ARTICLE 19, 19. Accessible at: https://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf.

ARTICLE 19 proposes three possible approaches for addressing the competing challenges and considerations posed by issues regarding intermediary liability:[29]

- **Hosts should not be liable for third party content (preferred model)**. ARTICLE 19 recommends that, in order to comply with international standards on freedom of expression, hosts should in principle be immune from liability for third party content in circumstances where they have not been involved in modifying that content. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body that has determined that the material at issue is unlawful. This provides for a much greater degree of legal certainty.
- **Notice-to-notice procedures (alternative model)**. ARTICLE 19 recognises that the preferred model might be too burdensome and costly for the courts to examine all applications for content removal given the high volume of requests that may be received. As an alternative, it is suggested that notice-to-notice procedures be developed as an alternative to notice and take down procedures. Such a system should meet the following conditions: (i) the notice sent by an aggrieved party should include minimum requirements, including the name of the complainant, the statement concerned and why it is considered unlawful, the location of the material, and an indication of the time and date when the alleged wrongdoing was committed; (ii) if the notice complies with these requirements, the host will then be required to forward the notice electronically as soon as is practicable (for example, within 72 hours) to the person identified as the wrongdoer, identified directly by the complainant, who must then decide whether to take the matter to a court or other independent body. If the alleged wrongdoer fails to respond or file a counter-notice within the required time limit, the host has a choice to take the material down or to decide not to remove it. In in the latter case, the host may be held liable for the content at issue if the complainant wishes to take the matter to a court or other independent body.
- **Content removal in cases of alleged serious criminality (model for specific cases)**. ARTICLE 19 further recognises that notice-to-notice systems may not be appropriate for all types of content, such as child sexual abuse images or incitement to violence, which are prohibited under international law. In such circumstances, the complainant should notify law enforcement of the suspected criminal activity, or alternatively notify the host who in turn should notify law enforcement. If the law enforcement authorities decide that the complaint is not urgent, they should seek a court order. Alternatively, if it is considered urgent – for example, if a person's life is at risk – ARTICLE 19 suggests that law enforcement should be given statutory powers to order the immediate removal or blocking of access to the content at issue, subject to such order being confirmed by a court within a specified period of time.

[29] ARTICLE 19. 2013b. *Internet intermediaries: Dilemma of liability*. (London: ARTICLE 19). 16. Accessible at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

MANILA PRINCIPLES ON INTERMEDIARY LIABILITY

Source: https://www.manilaprinciples.org/principles

The Manila Principles on Intermediary Liability (the "Manila Principles") were developed to assist policy makers and intermediaries in developing, adopting and reviewing legislation, policies and practices that govern the liability of intermediaries for third party content. As noted in the introduction to the Manila Principles, all communication over the Internet is facilitated by intermediaries. As such, the policies governing the legal liability of intermediaries for the content of these communications have an impact on the rights of users. As stated further: "Uninformed intermediary liability *policies, blunt and heavy-handed regulatory measures, failing to meet the principles of necessity and proportionality, and a lack of consistency across these policies, has resulted in censorship and other human rights abuses by governments and private parties, limiting individuals' rights to free expression and creating an environment of uncertainty that also impedes innovation online."*

The principles are as follows:

- *Intermediaries should be shielded from liability for third party content.*
- *Content must not be required to be restricted without an order by a judicial authority.*
- *Requests for restrictions on content must be clear and follow due process.*
- *Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.*
- *Laws and content restriction policies and practices must respect due process.*
- *Transparency and accountability must be built into laws and content restriction policies and practices.*

For the African context, the ACHPR's Declaration of Principles on Freedom of Expression and Access to Information in Africa is instructive on the minimum norms and standards to be applied in the region with respect to how intermediary liability should be managed. Principle 39 aligns itself with the Manilla Principles to the extent that it provides against strict liability on intermediaries with respect to proactively monitoring or discriminating against user content, as well as providing for rights-based frameworks by which states may require that intermediaries restrict or remove content to fulfil public policy objectives. As a minimum threshold, intermediaries may, therefore, be compelled to restrict or remove content where a bona fides state request is:

1. Clear and unambiguous.
2. Imposed by an independent and impartial judicial authority, subject to sub-principle 5.
3. Subject to due process safeguards.
4. Justifiable and compatible with international human rights law and standards.
5. Implemented through a transparent process that allows a right of appeal.

3.3 The right to privacy and its relationship with cybercrimes, cybersecurity and surveillance

Inasmuch as technology and the Internet have enabled significant strides in the enjoyment of human rights, facilitated economic and human development, they are also used to commit serious and sophisticated crimes that have significant implications for preserving law and order, and human and national security. For many African states these threats to national and human security have formed the basis for the rush to enact and enforce cybercrimes and cybersecurity legislation, including expanding the state's powers of surveillance of citizens.

It should be noted that the introduction of measures which can provide safety and security for citizens both on the Internet and in the "real-world" context is an issue of serious import, and state actors are under a positive obligation to establish and enforce national frameworks and laws to this end. To discharge these obligations, state actors in Africa and across the world are increasingly building their capacity for communications surveillance as a means of pre-empting, investigating, as well as enforcing, national cybercrimes and security laws. In some parts of Africa, the acquisition and use of tools which prevent or impair the state's ability to perform this surveillance function is also prohibited, carrying serious consequences for citizens.

Whereas there may be legitimate reasons for the introduction of policy and laws which equip the state with the powers and means to monitor and investigate technology mediated crimes, including through the use of communications surveillance, they also have a responsibility to do so through rights respecting and fair regulatory frameworks which do not unduly restrict the use of technology itself.

At the first instance, how the right to privacy is framed is of direct relevance. Article 17 of the ICCPR states that:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks."

In guiding the interpretation of this right, in Article 17 of its General Comment No. 16, the UN Human Rights Committee stated its view that:

> "this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons'; and obligates state actors to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to protect this right."[30]

Notwithstanding, the Committee also recognises that the protection of privacy is necessarily relative,"[31] and that balancing the rights to privacy and/or protection of reputation with the rights to freedom of information and expression presents challenges. To this end, the principles of necessity and proportionality are of direct relevance. As with the right to freedom of expression, the surveillance of communications may only be justified when it is prescribed by law, is necessary to achieve a legitimate aim, and proportionate to the aim pursued.

[30] UN Human Rights Committee. 1988. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Accessible at: https://www.refworld.org/docid/453883f922.html.

[31] *Ibid*.

THE NECESSARY AND PROPORTIONATE PRINCIPLES

Source: https://necessaryandproportionate.org/principles

The Necessary and Proportionate Principles provide useful guidance on how international human rights law applies in the current digital environment, with a particular focus on communications surveillance and technologies, and would similarly find application in respect of cybersecurity measures.

In terms of **Principle 5**, *in order for a measure to be proportionate, the following must be established:*

- *There is a high degree of probability that a serious crime or specific threat to a legitimate aim has been or will be carried out.*
- *There is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought.*
- *Other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option.*
- *Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.*
- *Any excess information collected will not be retained, but instead will be promptly destroyed or returned.*
- *Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.*
- *The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.*

The Necessary and Proportionate Principles also propose the following safeguards:

- **Principle 6:** *Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.*
- **Principle 7:** *Procedures for due process that ensure that lawful procedures governing any interference with human rights are properly enumerated in law, consistently practised, and available to the general public.*
- **Principle 8:** *Those whose communications are under surveillance should be notified of a decision authorising the communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies. Delay in notification would only be justifiable if notification would seriously jeopardise the purpose for which the communications surveillance is authorised, or there is an imminent risk of danger to human life; and authorisation to delay notification is granted by a competent judicial authority; and the user affected is notified as soon as the risk is lifted as determined by a competent judicial authority.*
- **Principle 9:** *States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers or authorities. Furthermore, they should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance.*

Policies aimed at restricting the use of encryption measures or anonymity online can also be seen as a restrictive measure on the content that can be placed online. Encryption and anonymity are necessary tools for the full enjoyment of human rights online, and enjoy protection by virtue of the critical role they play in securing the rights to freedom of expression and privacy.[32] They create a zone of privacy to facilitate freedom of opinion and expression in circumstances where users do not want their identities to be publicly known, particularly where they have concerns that this will be subject to scrutiny or harassment. These measures can safeguard and advance privacy, free expression, political accountability, public participation and debate, and can assist users explore basic aspects of their identity, such as one's gender, religion, ethnicity, national origin or sexuality.[33] As such, laws or policies that impede these measures or make disclosure mandatory can have the resultant effect of those users no longer expressing themselves online, and should be tested to ensure that it is proportioned to the harm addressed through the requirement of disclosure.

In 2016 the UN General Assembly adopted the Resolution on the Right to Privacy in the Digital Age.[34] This resolution made clear that unlawful or arbitrary surveillance, the interception of communications, and the unlawful or arbitrary collection of personal data are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression, and may contradict the tenets of a democratic society, including when undertaken on a mass scale. The resolution calls on states to, among other things:

- Review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.
- Establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for state surveillance of communications, their interception and the collection of personal data.
- Provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.
- Develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organisations.

For the African context, The Declaration of Principles on Freedom of Expression and Access to Information in Africa provides clear guidance on the understanding and interpretation of the relationship between the right to privacy and communication surveillance which aligns with these frameworks.

Principle 40 recognises citizens' right to privacy and expands this to include the right to anonymity, as well as to use digital technologies such as encryption which secure the confidentiality of their communications and personal information from access by third parties.[35]

[32] Media Legal Defence Initiative. 2018, 42.

[33] *Ibid*.

[34] OHCHR. 2014. *The Right To Privacy in The Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*. Accessible at: https://digitallibrary.un.org/record/777869#record-files-collapse-header.

[35] ACHPR. 2019. Declaration of Principles on Freedom of Expression and Access To Information In Africa, 40(2). Accessible at: https://www.achpr.org/legalinstruments/detail?id=69.

The Declaration also goes further to:

- Provide against laws prohibiting or weakening encryption unless such laws are justifiable and conform to international human rights law and standards.[36]
- Prohibit indiscriminate and untargeted collection, storage and analysis of a person's communications.[37]
- Place a positive obligation on state actors to provide adequate safeguards for the right to privacy, including where justifiable targeted surveillance has been undertaken in crime prevention and the investigation and enforcement of laws for a legitimate aim.[38]

3.3.1 Data sovereignty and protection

Although linked directly to the right to privacy, the issue of personal data sovereignty and protection has become so significant to the discussions on how the data of users of the Internet is collected, processed, analysed and stored that it requires discussion.

Personal data refers to any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, psychological, mental, economic, cultural or social identity. Reams of personal data is collected through our use of ICTs. For instance, a user's personal data is collected every time a purchase is made online, when registering for email, or signing up to a particular online service or application. Furthermore, a user's behaviour is frequently monitored and tracked online even without their knowledge.[39] Data protection principles and practices are needed for users have confidence in both government and business, and to minimise state and corporate surveillance and data exploitation.[40]

There has recently been some impetus towards the enactment of data protection laws in Africa – driven in significant part in order to facilitate trade with other states, particularly member states of the EU following the coming into force of the EU's General Data Protection Regulation (GDPR) which has become the *de facto* standard for regulating this issue.[41] However, to date, only 18 out of the 55 African states have comprehensive data protection laws, not all of which have been fully operationalised. That said, other states have incorporated data protection principles and practices into other ICT laws and policies. There are also a number of African regional instruments that deal with data protection:[42]

- **African Union (AU) Convention on Cyber Security and Personal Data Protection, 2014.**[43] This instrument, which is designed to apply across the region, includes provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. The provisions relating to data protection are contained in Chapter II, and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. However, it has not yet entered into force. Article 36 requires that it be ratified by at least 15 countries, but at the time of publication it had only been ratified by four countries.[44] If it does enter into force, it presents the opportunity to become a binding standard for the enactment of data protection laws in Africa.

[36] *Op. cit.,* 40(3).

[37] *Op. cit.,* 41(1).

[38] *Op. cit.,* 41(2) and (3).

[39] Privacy International, 9.

[40] *Ibid*.

[41] EU. 2016. General Data Protection Regulation (GDPR) on *Intersoft Consultation*. Accessible at: https://gdpr-info.eu/.

[42] MLDI, 2018. 36-37.

[43] AU. 2014. *African Union Convention on Cyber Security And Personal Data Protection*. Addis Ababa: African Union. At present, it has been ratified by one state, and signed by a further ten states.

[44] AU. 2020. *African Union Convention on Cyber Security And Personal Data Protection*. [The status List] Addis Ababa: African Union.

- **Draft East African Community (EAC) Legal Framework for Cyberlaws, 2008.**[45] This instrument covers topics relating to data protection, electronic commerce, data security and consumer protection. It is not intended to be a model law, but instead provides guidance and recommendations to states to assist with informing the development of their laws. Data protection is dealt with briefly at paragraph 2.5 of the EAC Legal Framework.
- **Supplementary Act on Personal Data Protection within ECOWAS, 2010.**[46] This instrument in a similar vein to the AU Convention on Cybersecurity and Personal Data Protection, provides detailed conditions for the lawful collection and processing of personal information and the rights of data subjects. It is designed to be directly transposed into a domestic context among ECOWAS member states.
- **SADC Data Protection Model Law, 2013.**[47] This instrument is a model law that can be utilised in a national context by member states. It seeks to ensure the harmonisation of ICT policies, and recognises that ICT technology developments impact the rights and protection of personal data, including in government and commercial activities. In addition to setting out the conditions for lawful processing of personal information and the rights of data subjects, it also deals with whistle-blowing, providing that the data protection authority must establish rules giving authorisation for, and govern the whistleblowing system that preserves the data protection principles, including the principles of fairness, lawfulness, purpose specification, proportionality and openness.

PERSONAL DATA PROTECTION GUIDELINES FOR AFRICA: A JOINT INITIATIVE OF THE INTERNET SOCIETY AND THE COMMISSION OF THE AFRICAN UNION

Source: https://www.Internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

In May 2018 the Internet Society and the Commission of the AU launched the Personal Data Protection Guidelines for Africa. As noted, the Guidelines were developed in the context of rapid change in the scope and availability of online services in Africa.

Importantly, the Guidelines note that:

"To sustain trust in the data-driven economy, AU members must acknowledge the role personal data plays, and the economic forces it generates. When successful, the data-driven economy can create economic growth, deliver compelling and innovative services, and improve the quality of life.

However, the data-driven economy can also have a dark side, where personal data is handled in exploitative or abusive ways, and where the interests of the data subject are damaged. The cost and risk inherent in these cases sometimes only becomes apparent when things go wrong – when there is a data breach, or fraud is exposed. This can have a profound effect on trust and confidence in online services, and a corresponding impact on the data-driven economy. The Guidelines recommend steps to reduce the risk of these latter, unwelcome outcomes."

[45] EAC & UNCTAD. 2018. EAC Framework for Cyberlaws. Accessible at: http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y.

[46] ECOWAS. 2013. Supplementary Act A1sa.1F01F10 On Personal Data Protection Within ECOWAS. Thirty-Seventh Session of the Authority of Heads of State and Government. Abuja: ECOWAS. Accessible at: http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

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

The Guidelines identify eight data protection principles that are common to most of the regional and domestic frameworks:

1. **Collection limitation**. *Personal data must be obtained and processed lawfully, fairly, and, to the extent possible, transparently.*
2. **Data quality**. *Personal data must be accurate at the point of collection, and reasonable steps must be taken to ensure its accuracy is maintained over the period of retention.*
3. **Purpose specification**. *Personal data must be collected only for specified, explicit, and legitimate purposes. Personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research.*
4. **Use limitation**. *Personal data must not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.*
5. **Security safeguards**. *Personal data should be protected by reasonable security safeguards to maintain its integrity and confidentiality.*
6. **Openness**. *There should be a general policy of openness about developments, practices and policies with respect to personal data.*
7. **Individual participation**. *Individuals must have the right to obtain information about their personal data held by others. This data must be provided within a reasonable period of time, in a form that is readily intelligible, and at a cost that is not excessive. Data subjects have the right to challenge their data and to have it amended if it is inaccurate, or erased if that is appropriate.*
8. **Accountability**. *Those who collect and process personal data must be able to demonstrate their compliance with these principles.*

Following its adoption in 2019, Principle 42 of the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa now provides for norms and standards by which state actors must provide for the protection and sovereignty of the personal data of persons, including placing a positive obligation on state actors to enact laws which protect and promote personal data protection and sovereignty.

As the collection, use and processing of personal data will be a likely component of most ICT activities, ICT policies developed in respect thereof should appropriately consider what data protection measures are required in order to safeguard the privacy and integrity of the data that they hold.

CHAPTER 4 GUIDING AND DRAFTING PRINCIPLES FOR ICT POLICIES

OBJECTIVES OF CHAPTER 1

In this chapter we will:

- Provide an overview of the guiding principles underpinning the information and communication technology (ICT) development process.
- Outline and describe the most significant steps in the ICT policy making cycle.

In chapter 4 we will discuss some general principles guiding the process and substantive features that make for the development of good ICT policy. We will consider some examples of where and how these principles have been applied.

4.1 Guiding principles

There are different guiding frameworks and approaches for the principles underpinning the ICT policy development process, as well as the broad outcomes they should produce. Every ICT governance instrument will need to be tailored to the specific technological strengths and the social and economic development priorities of the context in which it is being developed, taking into consideration its resources, capabilities and goals. Even though it is acknowledged that there is no one-size-fits-all approach, the following core principles should underpin the development and/or review process.

At the substantive level, the various legal instruments within the ICT governance framework should be informed from a user-centred and right-based perspective, be geared towards inclusivity, as well as be technologically appropriate. Regulatory certainty is important for all stakeholders, and serves to address fundamental challenges and improve conditions for investment. Importantly, ICT policies should be informed by a strong evidence base of the need, utility and practicality of the interventions under consideration, supported by appropriate research and data. This should typically be contained in an extensive regulatory impact assessment, and form the rational basis for further state action in its ICT infrastructure and policy development programmes. The following general principles are of relevance:

CONSTITUTIONALITY

Proposed laws, policies and regulations must comply with the prevailing constitutional framework as well as human rights and public international law. The rights of all parties must be balanced against one another and any limitations on those rights – including the right to freedom of expression, access to information or privacy – may only be enacted there they strictly comply with the three-part test for a justifiable limitation.

CONTEXT

Legal instruments under development or review must be relevant to the context and needs in the country at the particular time. For instance, it must take into consideration user demands, availability of infrastructure and regulatory imperatives. To the extent possible, the legal instrument should not be tailored to specific technology that may become redundant as technological advances are made; rather, an effort should be made to future-proof the instrument to ensure that it can remain relevant for longer.

CONSULTATION

Public consultation with all relevant stakeholders is critical to an effective law or policy. This should not be treated as a mere box-ticking exercise, but rather as a meaningful opportunity to engage with all the members of the public who will be most directly affected by the legal instrument being developed or reviewed, and who have a first hand understanding of its implications. This should be extended to a wide range of stakeholders from different sectors and different regions, including academics, technical experts and civil society.

COHERENCE

Lawmakers must ensure that different laws covering the same or similar subject matter are coherent, applied consistently and rationalized. This is important for legal certainty. For example, definitions and terminology should be used consistently across all instruments; contents should not be unnecessarily duplicated; and different laws should not prescribe different penalties for the same or similar conduct.

COORDINATION

The development and implementation of ICT policies often involve more than one government department. This requires there to be appropriate coordination of, and effective communication channels between, all role players, to ensure efficiency in the process. The policy instrument must clearly designate the public authority that has overarching responsibility for its implementation, and which should be responsible for providing the necessary guidance on monitoring and evaluation, as well as reporting on progress in respect of its implementation.

CAPACITY

Many ICT policies often require particular expertise at the level of development as well as implementation. Policy makers should ensure that the relevant expertise is included through all phases of the development and implementation processes. Internally, government departments responsible for the development and implementation of the ICT policy should also ensure that there are adequate capacity building initiatives to develop the relevant expertise within the relevant government departments.

Illustration 5: Core principles underpinning the development and/or review of ICT policy
Source: Avani Singh, 2020

GENERAL PRINCIPLES FOR GUIDING THE DEVELOPMENT OF ICT POLICY

Source: African Technology Policy Studies Network. 2002. A blueprint for developing national ICT policy in Africa: https://atpsnet.org/wp-content/uploads/2017/05/special_paper_series_5.pdf

The development of a specific ICT policy could be guided by the following general principles:

- *The policy should recognise and contribute to the realisation of the stated socio-economic development vision of the country, as well as contribute to the achievement of the relevant missions and strategies identified for the attainment of the vision.*
- *The policy should, as far as possible, address the cost, budgetary and resource requirements, allocation and mobilisation implications of the programmes, and the initiatives identified for implementation under the policy.*
- *Efforts should be made to introduce a structure into the plan by sub-dividing it into sub-components, each addressing a broad area of policy, such as infrastructure development or skills development.*
- *The various programmes, initiatives and packages identified for implementation should be practical, realistic and implementable, with clearly stated time-bound measurable targets.*
- *Targets that are set for the various programmes and initiatives should, where appropriate, be based on baseline study data on the status of relevant key socio-economic and ICT-related indicators.*
- *The policy should take into account the fact that the government will continue to formulate and implement its short- to medium-term socio-economic development and budgetary plans during the lifespan of the policy. In this respect, the policy should not be aimed at substituting this exercise. Rather, it should serve as a policy reference point which provides a complementary framework for facilitating government's long-term goal towards the development of an information and knowledge-based economy and society.*
- *The policy should incorporate elements of risk analysis that take into account the socio-economic development risks involved in implementing or not implementing the specific aspects of each sub-component of the policy.*
- *The policy should incorporate a programme monitoring and evaluation mechanism that allows for appropriate intervention procedures and actions with clear guidelines (where appropriate) on how and when these can be activated, and by which agency or authority.*
- *The policy should, as far as possible, be flexible enough to allow for modification, revision and adaptation as the need arises during implementation.*
- *In order to build flexibility into its implementation the policy should, as far as possible, avoid going into specific implementation details relating to its programmes and initiatives. The premise is that, for each programme or initiative, details should be developed and worked out during the actual implementation of the policy to take into account specific circumstances, constraints, opportunities and developments. This approach will also allow for the fine-tuning of the programme details as the need arises during the implementation of the policy.*

4.2 The ICT policy making process

The policy making process will always vary according to the laws, norms and standards that have been set in place in the contexts where they must apply. However, there are four broad steps in the policy making cycle which support the formulation of effective and responsive regulatory instruments: (i) agenda setting; (ii) formulation and adoption; (iii) implementation; and (iv) evaluation and termination. These steps and their significance in the cycle are discussed below.

4.2.1 Step 1: Agenda setting

The agenda setting function is usually a highly technical exercise that requires conceptual clarity on the contextual issues seeking the policy intervention, the required outcomes and the tools and conditions required to facilitate them. It often starts with a contextual enquiry which requires the identification of a problem or a series of challenges related to the policy object. This might happen from the ground up, where the parties experiencing these challenges present them to the policy making authority for specific intervention, or it might be directed by the policy making authority itself based on its analysis of the circumstances under its responsibility. For example, private sector role players may motivate for stronger cybercrime investigation and prosecution capacity to combat fraud on mobile money platforms; or civil society groups working in the area of sexual and gender-based violence may desire frameworks to combat cyber harassment and technology mediated violence against women.

This step often requires engagement with subject matter specialists and the relevant authorities to provide perspective on what is and isn't available to the policy making authority to produce the desired policy outcomes. It is produced through a variety of tools deployed at different fora. This may include advocacy at the state or regional levels; the development of position papers and concept notes; research reports; consultations with, and open letters to, state representatives; as well as through strategic litigation.

The challenges and their context often take time to identify, and benefit from scoping or mapping exercises to determine their full purview as well as the direct and indirect challenges that need to be resolved. Challenges initially identified may develop with stakeholder input, and will benefit from consultation with affected parties and people with technical expertise or industry-specific knowledge, including technology companies and service providers.

4.2.2 Step 2: Formulation and adoption

Once a problem has been identified and the various issues and necessary approaches to respond to them are sufficiently ventilated, an ICT or related policy will need to be formulated and adopted. A guide to drafting an ICT policy is detailed in 4.3 below. ICT policy formulation should be a broad and extensive consultative process which should be developed through a series of stakeholder engagements. Its primary purpose is to determine the approach that needs to be followed to most effectively realise the solutions to the identified problem, and it should be forward looking in its orientation. This must include defining policy harmonisation programmes, setting realistic timeframes for implementation, and stating the conditions which would give rise to the conclusion of the policy statement's applicability, as appropriate.

Central to ICT policy formulation is public participation and citizen-led accountability initiatives.[1] Engaging with and understanding the challenges faced by individuals, civil society organisations (CSOs), technology businesses, industry actors, and organs of the state assists not only with agenda setting but also the appropriate determination of suitable approaches to resolving ICT challenges. In order to be successful, public participation processes require suitably trained professionals to ensure that they are run smoothly and properly facilitated. They can take the form of requests for written comments, in-person

[1] Tshoose, C.I. 2015. Dynamics of Participation in Local Government: A South African Perspective. *African Journal of Public Affairs*, Vol. 8, 12 onwards. Accessible at: https://repository.up.ac.za/handle/2263/58158.

or e-consultations, training and facilitation workshops, or a combination of the above. They are most effective when all stakeholders are properly briefed on the intended objectives and outcomes, based on the identified challenges.

Public participation is meant to be robust. Contradictory proposals are often made by a variety of actors with distinct and divergent interests. Skilled policy makers should welcome these engagements as an aid to understanding the totality of challenges faced and interests pursued, and as a tool to ensuring effective ICT policy formulation and the avoidance of policy uncertainty, which may give rise to unforeseen social and economic consequences. Effective ICT policy may also require the harmonisation and alignment of multiple laws, regulations, and procedures.

Once an ICT policy instrument has been formulated it needs to be adopted at either the executive or legislative level. Adoption, and the appropriate fora for adoption, will largely depend on the nature of the ICT policy instrument. It may be submitted to Parliament, Congress or the relevant ministry; and may, in some instances, be confirmed, modified, or rejected by a court. Prior to adoption, policy makers should ensure that adequate steps have been taken to ensure that a broad and consultative process was led and that the policy contains appropriate and effective accountability mechanisms.

4.2.3 Step 3: Implementation

Once the ICT policy has been adopted, it needs to be implemented. To the extent that the policy has followed proper agenda setting, formulation, and adoption processes, realistic and effective implementation strategies should have already been considered. Key organs, ministries, agencies, and stakeholders should already have been identified, and implementing documentation such as guidelines, frameworks, and implementation plans, based on realisable timeframes, prepared. Importantly, public awareness and buy in may need to be enhanced during the implementation phase which may benefit from a collection of user friendly and technical documents. Extensive awareness and training campaigns may also be needed where the behavioural change of users, particularly in the ICT policy space, is necessary for full realisation of the policy objectives.

ICT policy implementation, which is detailed in 4.3, below, is often carried out by institutions other than those who formulated the policy. Resultantly, these institutions should be fully engaged through the policy drafting process, and appropriate compliance and enforcement mechanisms should be established to ensure that the policy remains effective and realisable regardless of administrative changes.

4.2.4 Step 4: Evaluation and termination

Throughout the course of implementation the effectiveness of the ICT policy instrument must be monitored and evaluated. Evaluation is complex and multi-faceted, and is used to determine whether the policy is solving the challenges identified and what, if any, unintended consequences have been caused. Evaluation should consider changes to the initial agenda or challenges faced, whether the policy is appropriately formulated, and whether the implementation strategies identified are suitably matched to the achievement of the envisaged solution, goal, or objective.

Evaluation is often based on data and various types of analysis, including a cost-benefit analysis. Well drafted polices will often include “modes of evaluation” such as the realisation of goals or phases, and the intended results at defined periods in the implementation cycle.

Developing policies with clearly stated objectives, milestones and outcomes provides implementing authorities and agencies with a clear roadmap to achieving their respective and specific goals, as well as an indication of the key data they need to monitor and adjust their performance against in order to meet targets. Well drafted polices may include evaluation strategies which are determined during the formulation process.

Following evaluation, the life cycle of a policy may end, and may need to be terminated or replaced with a new policy. This may be occasioned by the realisation of the policy objectives, a failure of the policy to bring about the requisite change, or through public or private sector developments altering the need or utility of a policy.

This evaluation should be a critical analysis that meaningfully reviews the extent to which the desired outcomes have been attained. A useful way of doing this is through the development of indicators that can serve as a consistent measure, assessed at periodic intervals, to determine whether the implementation of the policy is proceeding on track.

THE DEVELOPMENT OF INDICATORS

A number of different organisations have developed indicators (or indices) in the context of, for example, digitisation, ICT development, network readiness and broadband development. These may be of assistance to policy makers when formulating ICT policies. The following examples of indicator frameworks can be adapted to the policy maker's specific context, and can find relevance throughout the policy process, from formulating the vision and objectives of the policy through to the monitoring and evaluation of the implementation.

The **International Telecommunication Union's (ITU's) ICT Development Index** *measures digitisation on the basis of six components, each of which are further broken down into sub-components and sub-subcomponents. The components and sub-components are as follows:*

1. **Affordability**. *Residential fixed line cost; mobile cellular cost; fixed broadband Internet access cost.*
2. **Infrastructure reliability**. *Investment per telecom subscriber (mobile, broadband and fixed).*
3. **Network access**. *Network penetration; coverage, infrastructure and investment.*
4. **Capacity**. *International Internet bandwidth (kbit/s per user); percentage of broadband connections higher than 2 mbit/s.*
5. **Usage**. *Internet retail volume; e-government usage; percentage of individuals using the Internet; data as a percentage of wireless average revenue per user; dominant social network unique visitors per month per capita; SMS usage.*
6. **Human capital**. *Percentage of engineers in the labour force and of skilled labour.*

UNESCO's Internet Universality Indicators[2] *also provide a framework for assessing Internet development. The indicators are based on the ROAM-X categories to assess Internet universality at the level of a national Internet environment:*

- **Rights**. *Policy, legal and regulatory framework; freedom of expression; right of access to information; freedom of association and the right to take part in public affairs; the right to privacy; social, economic and cultural rights.*
- **Opennes**s. *Policy, legal and regulatory framework; open standards; open markets; open content; open data and open government.*
- **Accessibility to all**. *Policy, legal and regulatory framework; connectivity and usage; affordability; equitable access; local content and language; capabilities and competencies.*
- **Multi-stakeholder**. *Policy, legal and regulatory framework; national Internet governance; international and regional Internet governance.*
- **X – Cross-cutting**. *Gender; children; sustainable development; trust and security; legal and ethical aspects of the Internet.*

[2] UNESCO. 2018. Defining Internet Universality Indicators. Second Draft. Paris: UNESCO. Accessible at: https://en.unesco.org/sites/default/files/unesco_Internet_universality_indicators_second_version.pdf.

4.3 A guide to drafting an ICT policy

Flowing from the overview of the ICT policy making process, the formulation stage in general, and drafting ICT policy in particular, is central to the success or otherwise of an ICT policy. General principles apply to the formulation of ICT policy and are discussed below.

4.3.1 Use of plain language

As discussed in the previous chapters, ICT language is complex, and concepts are often foreign to beneficiaries, stakeholders, and policy makers themselves. In consultation with technical experts, policy drafters should ensure that ICT policies are drafted in plain language and in a manner that guards against ambiguity and uncertainty. Simplifying ICT language for broader consumption is central to effective formulation and implementation. Primary policy documents should be clear, but as short as possible, and should be complemented by technical documentation to ensure effective implementation.

4.3.2 The policy statement

Related to the policy title, the policy statement should be a brief statement of the identified challenges and key targets, goals, and objectives of the policy. Specific details should be omitted but the statement should contain sufficient information for a reader to understand the purpose of the policy and the challenge it seeks to resolve.

4.3.3 Definitions

All terminology used in the policy, including the acronyms that are common in the ICT space, should be defined at the outset. Effective policies may include an extensive glossary of terms, similar to the glossary found at the beginning of this handbook. Attention should be paid to carefully defining and circumscribing the key terms used throughout the policy to avoid ambiguity and uncertainty.

4.3.4 Application

Following the definitions sections, a section on the application of the policy should be included. This section should detail what the policy targets are and to whom it applies.

4.3.5 Intended objectives and outcomes

In addition to the core content, a policy should expressly list the intended objectives and the applicable outcomes for each goal or phase. The intended objectives and outcomes should be sufficiently detailed to allow for intervention, where necessary, by enforcement mechanisms in the event that a policy is not properly implemented.

SOUTH AFRICA CONNECT: CREATING OPPORTUNITIES, ENSURING INCLUSION – SOUTH AFRICA'S BROADBAND POLICY, 2013

Source: https://www.gov.za/documents/electronic-communications-act-south-africa-connect-creating-opportunity-ensuring-inclusion

South Africa Connect is South Africa's national broadband policy, with its associated strategy and plan, that seeks to achieve "a seamless information infrastructure by 2030 that will underpin a dynamic and connected vibrant information society and a knowledge economy that is more inclusive, equitable and prosperous". The objectives are set out in section 3, and include the following:

a. Affordable broadband available nationally, to meet the diverse needs of public and private users, both formal and informal, consumers and citizens.

b. Policy and regulatory conditions that enable public and private sector players to invest and also contribute in other ways to reaching South Africa's broadband ambitions.

c. Efficient public sector delivery, including e-government services, underpinned by the aggregation of broadband needs.

d. All public institutions at the national, provincial and municipal level should benefit from broadband connectivity, and this should be extended to the communities they serve.

e. A framework within which public and private enterprises, formal and informal, are able to fully exploit the efficiencies offered by ubiquitous broadband and its potential for innovation.

f. The development of a strong national skills base so that South Africa can perform as a proficient and globally competitive knowledge economy.

g. A vibrant creative and software industry that produces content and applications that are relevant and meet the needs of the diverse users in the country.

h. A literate and skilled society that can effectively access services and content, including public information and public services.

4.3.6 Core content

The core content of a policy should clearly outline the steps to realisation of the vision of the policy instrument, resources needed, time frames, stakeholders, and the strategies to resolve the identified challenges. Some of the more significant rights-based themes in ICT policy drafting have been identified in Chapter 3 and can assist the user in determining an appropriate structure and content needed to draft an ICT policy that responds to them appropriately.

4.3.7 Time-frames and modes of evaluation

Alongside the intended objectives and outcomes, a policy should expressly indicate applicable time-frames and the modes of evaluation for each goal or phase. Timelines and modes of evaluation assist all stakeholders and implementing teams better understand the envisioned process and legislative, capacity and resource requirements needed to achieve each of the specific objectives and outcomes.

4.3.8 Related laws, regulations, and procedures

Importantly, effective policies anticipate the raft of laws, regulations, and procedures that may need to be developed, harmonised, or aligned to ensure that the regulatory landscape is suitable to the effective implementation of the policy. Relevant laws, regulations, or procedures should therefore be listed in the policy itself to assist implementation teams, legislators, and policy makers identify roles and responsibilities in effective legislative and regulatory harmonisation.

4.3.9 Policy implementation

Following the formulation of a policy, implementation is often the stumbling block to meeting, and delivering on, the identified agenda. This is often as a result of a lack of technical expertise, resources, and genuine political will, or as a result of overly ambitious or ill-defined objectives. The considerations below are useful to policy makers in conceptualising not only the agenda and the formulation of an ICT policy, but also the skills, expertise, and mechanisms needed for effective ICT policy implementation.

4.3.10 Skills development and technical expertise

The complexities associated with ICT policy making are enormous. Oftentimes, ICT policy is formulated and drafted by people with technical expertise, and then it is left to civil servants with varying degrees of competence and proficiency concerning the subject matter to implement. Challenges such as cybercrime and universal access are complex, often requiring skilled personnel with both specific as well as multi-disciplinary competence to facilitate effective implementation. ICT policies should include skills development programmes, and should be managed by people with the necessary technical expertise.

KENYA NATIONAL INFORMATION AND COMMUNICATIONS (ICT) POLICY, 2016

Source: http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf

The Kenya National ICT Policy, 2016 is an example of a comprehensive national ICT policy. Following a decade after the ICT policy of 2006, it was necessitated by changes that occurred in the ICT landscape.

Notably, the policy identifies ten key guiding principles: (i) constitutional principles and values; (ii) technology and convergence; (iii) universal service; (iv) open access; (v) competition; (vi) innovation; (vii) standards; (viii) internationalisation, national cohesion and integration; (ix) privacy and security; and (x) recognition of the United Nations Sustainable Development Goals (UN SDGs).

The policy notes further that the realisation of these principles will depend on the adequacy and availability of the skilled human resource capacity. Accordingly, the policy provides that the government will support the creation of the necessary capacity by:

- *Integrating IT subjects in the curriculum at all levels of education.*
- *Establishing educational networks for sharing educational resources and promoting e-learning at all levels.*
- *Facilitating public-private partnerships to mobilise resources in order to support e-learning initiatives.*
- *Promoting the development of integrated e-learning curriculum to support ICT in education.*
- *Promoting distance education and virtual institutions, particularly in higher education and training.*
- *Facilitating sharing of e-learning resources between institutions.*
- *Exploiting e-learning opportunities to offer Kenyan education programmes for export.*
- *Integrating e-learning resources with other existing resources.*

- *Encouraging the establishment of ICT Centres of Excellence.*
- *Encouraging and supporting ICT training for decision makers, community and civil society leaders.*
- *Creating opportunities and providing assistance for the disadvantaged, people with special needs, women and the youth to acquire IT skills.*
- *Enhancing capacity for research and development in ICT.*
- *Introducing incentives and measures to improve training in broadcasting and the media to ensure qualitative and quantitative growth of the broadcasting sector.*
- *Encouraging national professional bodies for media practitioners to participate in setting standards in broadcasting, and encouraging media training institutions to provide structured specialised programmes that cater for people with talent for creative writing, film production, animation creative and technical aspects of broadcasting.*
- *Engaging women, youth and children, communities in underserved areas, and other disadvantaged groups, including people with disabilities, through e-inclusion and e-accessibility activities and programmes.*
- *In order to have global competitiveness of ICT products and services, encouraging universities to establish post-doctoral research fellow positions on contractual and attractive terms in order to attract world-class researchers.*

As noted in the policy: "Kenya is not the only country with insufficient numbers of skilled and experienced experts in ICT and in other professions that rely on ICT. It is therefore necessary to view Kenya's human capital needs in the global context. Hard choices must be made between importing needed skills, and slowly nurturing them within the country. Other choices are needed on the priorities of realigning the educational and vocational training pipelines to meet the needs of our labour markets."

These principles, and the levers identified to build the capacity necessary for the realisation of these principles in the ICT landscape, should be taken into consideration in the development of any national ICT policy, as they find relevance in practically every jurisdiction.

4.3.11 Institutional separation and coordination

Effective ICT polices often establish or delegate implementation authority to institutions other than those responsible for developing the policy instrument. Alternatively, institutions may be established as a result of a policy instrument. This institutional separation often takes place to ensure that institutions most capable of effective implementation are in charge of the implementation process. In the ICT space, multiple institutions, regulators, authorities, or working groups, both existing and newly-established, may be jointly charged with policy implementation, requiring enhanced coordination and communications systems. All relevant institutions should be consulted during the agenda setting and formulation and adoption steps to ensure that they have sufficient time to budget, increase capacity, and establish skills development programmes. Indeed, these factors should already be factored into the regulatory impact assessment and refined throughout the policy development process. Further, a clear understanding of what each institution's roles and responsibilities are, and how they interact with and relate to one another, should be established.

SOUTH AFRICA NATIONAL CYBERSECURITY POLICY FRAMEWORK, 2015

Source: https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000

The National Cybersecurity Policy Framework was "intended to implement an all-encompassing approach pertaining to all the role-players (State, public, private sector, civil society and special interest groups) in relation to cybersecurity". Accordingly, it sets out the role to be played in the context of cybersecurity by several government departments and agencies:

- **The Department of Justice and Constitutional Development and the National Prosecuting Authority**. *They were given overall responsibility for facilitating cybercrime prosecution and court processes in accordance with the applicable laws.*
- **The Ministry of State Security and the State Security Agency**. *They were given overall responsibility and accountability for coordination, development and implementation of cybersecurity measures in the country as part of the national security mandate.*
- **The Department of Police and the South African Police Service**. *They were given overall responsibility for the prevention, investigation and combating of cybercrime in the country – including the development of cybercrime policies and strategies – and providing for specialised investigative capacity and interaction with national and international stakeholders.*
- **The Department of Telecommunications and Postal Services**. *It was given overall responsibility for developing and implementing policies, regulations and industry standards regarding the ICT aspects, and to establish the National Cybersecurity Advisory Council and the Cybersecurity Hub.*
- **The Department of Defence and Military Veterans**. *It was given overall responsibility for coordination, accountability and implementation of cyber defence measures in the country, and to develop policies and strategies in this regard.*
- **The Department of Science and Technology**. *It was given the responsibility for the development, coordination and implementation of national capacity development programmes.*

As stated further, all other organs of state would be required to align their policies and practices with the National Cybersecurity Policy Framework insofar as they might relate to cybersecurity.

4.3.12 Guidelines, frameworks and implementation plans

In order to ensure effective implementation, a series of technical documents should be formulated and drafted, alongside the ICT policy. Subject to the dictates of a particular policy, these documents may include:

- **Operational guidelines**. These should detail, in broad terms, steps to realise the agenda dictated in the policy.
- **Frameworks**. These may provide additional information not contained in the policy for use by implementation teams.
- **Implementation plans**. These may seek to expand on the objectives, outcomes, and timeframes specified in a policy, including metrics for evaluation.
- **Technical specifications**. These should assist experts with implementing the technical aspects necessary to realise the agenda.

IMPLEMENTATION PLAN FOR THE NATIONAL BROADBAND POLICY FOR RWANDA, 2013

Source: http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_Polices/National_Broadband_Policy.pdf

The National Broadband Policy for Rwanda contains an implementation plan, which specifies the activities, targets, responsible institution, the estimated timing of the activity, and the estimated costs. Short-term measures are anticipated to be completed within a two-year period, with longer-term measures within a five-year period.

For example, the activities include:

Activity: Creation of a public-private partnership / wholesale company

Timeline: Ongoing

Responsible entity: Ministry of Youth and ICT; Rwanda Development Board

Estimated cost: Existing operational expenses

Activity: Issuance of wholesale licences

Timeline: Ongoing

Responsible entity: Ministry of Youth and ICT; Rwanda Utilities Regulatory Authority

Estimated cost: Operational expenses

Activity: Review frequency bands to allow efficient deployment of technologies

Timeline: October 2013

Responsible entity: Rwanda Utilities Regulatory Authority

Estimated cost: None

The implementation plan states further that it is proposed to be updated annually, with revisions to be based on the actual progress made each year.

4.3.13 Public awareness, education and training

In pursuing any policy agenda or objective in the ICT space, behavioural change by ICT users or beneficiaries may be necessary for the effective implementation of the policy and to the realisation of its objectives. Public awareness campaigns, education, and training should therefore be central to implementation strategies and to assuring that objectives are met.

4.3.14 Measuring compliance

ICT policies often envisage multiple complex processes, based on multiple legislative and regulatory instruments. Sufficient monitoring mechanisms and targets, based on the objectives, outcomes, and timeframes dictated in a policy, are therefore necessary for enhanced coordination between implementation teams and the realisation of interim goals and strategies, and the effective implementation of the policy as a whole.

NIGERIA NATIONAL BROADBAND PLAN 2013-2018, 2013

Source: https://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf

According to the National Broadband Plan, the broadband vision for Nigeria "is one of a society of connected communities with high speed Internet and broadband access that facilitate faster socio-economic advancement of the nation and its people". The National Broadband Plan notes further that: "For any plan to be effective, it must be monitored, and the success of the program evaluated". The National Broadband Plan sets out seven key performance indicators – measured on a quarterly basis, beginning with the baseline as at 31 January 2013, to be monitored and reported on by the Broadband Council. The indicators are intended to guide a coordinated programme for accelerated broadband expansion:

1. *Percentage of the national population with access to 3G/4G mobile Internet service.*
2. *Percentage of the national population with access to fixed broadband service.*
3. *Number of active public access points.*
4. *Average price of 3G/4G mobile Internet subscription.*
5. *Average price of fixed broadband Internet subscription.*
6. *Number of households in all major cities without broadband.*
7. *Average broadband speed.*

Additionally, the National Broadband Plan sets specific targets in the short-, medium- and long-term across three target types:

1. *Broadband targets for cities, comprising availability (coverage) and penetration (usage).*
2. *Broadband national targets, comprising availability (coverage) and penetration (usage).*
3. *Broadband targets for communities, comprising community public access venues through either a wired or wireless medium.*

4.3.15 Compliance and enforcement mechanisms

Effective ICT policies should identify and establish compliance and enforcement mechanisms. Compliance mechanisms assist stakeholders and implementation teams in meeting their obligations in terms of the policy. Enforcement mechanisms compel compliance in the event that stakeholders or implementation teams fails to comply with policy obligations. These mechanisms are central to ensuring that policy is citizen-led and empowers all rights-bearers to compel the state and other stakeholders to meet its stated objectives under the policy instrument.

The ability of rights-bearers to drive regulatory changes and enforce objectives is central to the effective functioning of a democracy. Enforcement or oversight mechanisms are therefore necessary to ensure social accountability in the implementation process. These mechanisms should be easy to access, and sufficiently capacitated to deal with complaints. Importantly, the decisions of these mechanisms should be binding on the institutions and agencies mandated to implement the policy instrument.

BIBLIOGRAPHY

Access Now. What is an Internet shutdown? Accessible at: https://www.accessnow.org/keepiton/?ignorelocale.

ACHPR. 1998. Media Rights Agenda, Constitutional Rights Project, Media Rights Agenda and Constitutional Rights Project v Nigeria. Accessible at: http://www.worldcourts.com/achpr/eng/decisions/1998.10.31_Media_Rights_Agenda_v_Nigeria.htm.

ACHPR. 2002. Declaration of Principles on Freedom of Expression in Africa, 32nd Session In University of Minnesota, Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia. Minnesota: University of Minnesota. Accessible at: http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html.

ACHPR. 2016. 362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016. Banjul: ACHPR. Accessible at http://www.oas.org/en/sla/dil/docs/acceso_informacion_desarrollos_UA_ACHPR-Res_362_LIX_2016.pdf.

ACHPR. 2019. Declaration of Principles on Freedom of Expression and Access To Information In Africa. Accessible at: https://www.achpr.org/legalinstruments/detail?id=69.

Adeleye, N. & Eboagu, C. 2019. Evaluation of ICT development and economic growth in Africa. Netnomics. 20: 31–53. Accessible at: https://doi.org/10.1007/s11066-019-09131-6.

African Technology Policy Studies Network. 2002. A blueprint for developing national ICT policy in Africa. Accessible at: https://atpsnet.org/wp-content/uploads/2017/05/special_paper_series_5.pdf.

ARTICLE 19. 2013a. Freedom of Expression and ICTs: Overview of International Standards. London: ARTICLE 19. Accessible at: https://www.article19.org/data/files/medialibrary/37380/FoE-and-ICTs.pdf.

ARTICLE 19. 2013b. Internet intermediaries: Dilemma of liability. London: ARTICLE 19. Accessible at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

ARTICLE 19. 2016. Freedom of Expression Unfiltered: How Blocking And Filtering Affect Free Speech. London: ARTICLE 19. Accessible at: https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf.

Association for Progressive Communications. 2009. 'The APC ICT Policy handbook', p7. Accessible at: https://www.apc.org/sites/default/files/APCHandbookWeb_EN_0.pdf.

Association for Progressive Communications. 2014. Frequently asked questions on Internet intermediary liability. Accessible at: https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-Internet-intermed.

AU. 1990. African Charter on the Rights and Welfare of the Child. Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-charter-rights-and-welfare-child.

AU. 2007. African Charter on Democracy, Elections and Governance. Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-charter-democracy-elections-and-governance.

AU. 2013. Agenda 2063: The Africa We Want. (Popular version) Addis Ababa: African Union. Accessible at: https://au.int/en/Agenda2063/popular_version.

AU. 2014. African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

AU. 2020. African Union Convention on Cyber Security and Personal Data Protection. [The status List] Addis Ababa: African Union. Accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Blimpo, M.P. et. al. 2017. Leapfrogging: The Key to Africa's Development-from Constraints to Investment Opportunities. Washington, D.C: World Bank Group. Accessible at: http://documents.worldbank.org/curated/en/121581505973379739/Leapfrogging-the-key-to-Africas-development-from-constraints-to-investment-opportunities.

Chakravorti, B. & Chaturvedi, R.S. Research: How Technology Could Promote Growth in 6 African Countries. Havard Business Review. Accessible at: https://hbr.org/2019/12/research-how-technology-could-promote-growth-in-6-african-countries.

Chavula, H.K. & Chekol, A. 2011. ICT policy development process in Africa. In Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements (IGI Global).

Comninos, A. 2012. The liability of Internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain. Johannesburg: APC.

CIPIT. 2018. International Internet Disruption in Africa: Estimating Impact in Observable and Shadow Economies. Nairobi: Strathmore University. Accessible at: https://cipit.strathmore.edu/wp-content/uploads/2020/05/PDF-3.pdf.

Creative Commons License. Accessible at: https://creativecommons.org.

Dahir, A.L. 2018. Cameroon Is Being Sued for Blocking The Internet in its Anglophone Regions. Quartz Africa. Accessible at: https://qz.com/africa/1192401/access-now-and-Internet-sans-frontieres-suecameroon-for-shutting-down-the-Internet/.

Department of Communications and Digital Technologies. 2013. South Africa Connect: Creating Opportunities, Ensuring Inclusion – South Africa's Broadband Policy. Accessible at: https://www.gov.za/documents/electronic-communications-act-south-africa-connect-creating-opportunity-ensuring-inclusion.

EAC & UNCTAD. 2018. EAC Framework for Cyberlaws. Accessible at: http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y.

EACJ. 1998. Treaty for the Establishment of the East African Community. Accessible at: https://www.eacj.org/?page_id=33#toc-article-6-fundamental-principles-of-the-community.

EACJ. 2015. Burundi Journalists' Union v The Attorney General of the Republic of Burundi, Reference No. 7 of 2013. Accessible at: http://eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi.

ECOWAS. 1975. Economic Community of West African States (ECOWAS) Revised Treaty. In UiO The Faculty of Law. Accessible at https://www.jus.uio.no/english/services/library/treaties/09/9-01/ecowas_treaty_revised.xml.

ECOWAS. 2013. Supplementary Act A1sa.1F01F10 On Personal Data Protection Within ECOWAS. Thirty-Seventh Session of the Authority of Heads of State and Government. Abuja: ECOWAS. Accessible at: http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

Electronic Frontier Foundation. 2020. Manila Principles on Intermediary Liabilities. Accessible at: https://www.manilaprinciples.org/principles.

EU. 2016. General Data Protection Regulation (GDPR) on Intersoft Consultation. Accessible at: https://gdpr-info.eu/.

Fielden, L. 2012. Press regulation: Taking account of media convergence', Foundation for Law, Justice and Society. England: University of Oxford. Accessible at: http://www.fljs.org/sites/www.fljs.org/files/publications/Fielden.pdf.

Geelen, M. 2016. Cyber securitization and security policy: The impact of the discursive construction of computer security on (national) security policy making in the Netherlands, 1. Accessible at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/53654/2016_Geelen_CSM.pdf?sequence=1.

Gillwald, A. 2015. ICT4D, Regulation and Strategy. The International Encyclopaedia of Digital Communication and Society: 1-11.

Wasserman, H. & Madrid-Morales, D. 2019. An Exploratory Study of "Fake News" and Media Trust in Kenya, Nigeria and South Africa, African Journalism Studies. 40:1, 107-123, Accessible at: https://doi.org/10.1080/23743670.2019.1627230.

Hern, A. 2020a. Tech Firms Like Facebook Must Restrict Data Sent from EU to US, Court Rules. The Guardian. 16 July. Accessible at: https://www.theguardian.com/technology/2020/jul/16/tech-firms-like-facebook-must-restrict-data-sent-from-eu-to-us-court-rules.

Hern, A. 2020b. Facebook Says It May Quit Europe Over Ban on Sharing Data with US. The Guardian. 22 September. Accessible at: https://www.theguardian.com/technology/2020/sep/22/facebook-says-it-may-quit-europe-over-ban-on-sharing-data-with-us.

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

Human Rights Law in Africa, 2004a. Treaty of The Economic Community of West African States (Ecowas) [Revised]. Human Rights Law in Africa Online. 1(1):648-653. Accessible at: https://doi.org/10.1163/221160604X00431.

Human Rights Law in Africa, 2004b. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. Human Rights Law in Africa Online. 1(1):818-822. Accessible at: https://doi.org/10.1163/221160604X00954.

Iiori, T. & Killander, M. Internet shutdowns in Africa threaten democracy and development. The Conversation. Accessible at: https://theconversation.com/Internet-shutdowns-in-africa-threaten-democracy-and-development-142868.

Internet Society. 2018. Policy Brief: Internet Shutdowns. 18 December. Accessible at: https://www.Internetsociety.org/policybriefs/Internet-shutdowns.

ITU. 2018a. ICTs for a Sustainable World #ICT4SDG. Geneva: ITU. Accessible at: https://www.itu.int/en/sustainable-world/Pages/default.aspx.

ITU. 2018b. Regulatory Challenges and Opportunities in the New ICT Ecosystem. Geneva: ITU. Accessible at: https://www.itu-ilibrary.org/science-and-technology/regulatory-challenges-and-opportunities-in-the-new-ict-ecosystem_pub/81118c75-en.

ITU. 2018c. The Economic Contribution of Broadband, Digitization and ICT Regulation Geneva: ITU. 1. Accessible at: https://www.itu.int/pub/D-PREF-EF.BDR-2018.

ITU. 2019. Measuring Digital Development: Facts and Figures. Geneva: ITU. Accessible at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

Iyer, N. et. al. 2020. Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet. Accessible at: https://www.apc.org/sites/default/files/Report_FINAL.pdf.

Kashorda, M & Waema, T. 2014. E-readiness Survey of Kenyan Universities 2013. Ministry of Information and Communication Technology. Accessible at: http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf.

Kofi Annan Foundation. 2020. Protecting Electoral Integrity in the Digital Age: The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age. Accessible at: https://storage.googleapis.com/kofiannanfoundation.org/2020/05/85ef4e5d-kaf-kacedda-report_2020_english.pdf.

Kuyoro, S.O. 2012. ICT: an effective tool in human development. International Journal of Humanities and Social Science. 2(7):157-162.

Manancourt, V. 2020. Top Facebook exec pushes back on talk of Europe withdrawal. Politico. 23 September. Accessible at: https://www.politico.eu/article/nick-clegg-top-facebook-executive-pushes-back-on-talk-of-europe-withdrawal/.

Media Legal Defence Initiative. 2018. Training Manual on Digital Rights and Freedom of Expression Online. (London: Media Legal Defence Initiative), 4. Accessible at: https://www.mediadefence.org/resources/mldi-training-manual-on-digital-rights-and-freedom-of-expression-online/.

Mohamed, M.S. et. al. 2010. Information and Communication Technology (ICT) Policy: A Quantitative Assessment for Sustainable Development. Journal of Information & Knowledge Management. 9(03):227-239.

Mozilla Foundation. Accessible at: https://www.mozilla.org/en-US/moss/.

National Broadband Policy for Rwanda. 2013. Accessible at: http://minict.gov.rw/fileadmin/Documents/Policies_and_Rugulations/ICT_Polices/National_Broadband_Policy.pdf.

Nigeria National Broadband Plan 2013-2018. 2013. Accessible at: https://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf.

OHCHR. 2014. The Right To Privacy in The Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. Accessible at: https://digitallibrary.un.org/record/777869#record-files-collapse-header.

Open Technology Fund. Accessible at https://www.opentech.fund.

SADC. 2001. Protocol on Culture, Information and Sport 2001. Blantyre: SADC. Accessible at: https://www.sadc.int/documents-publications/show/797.

Salmon, E. 2016. 'Independent regulation of broadcasting: A review of international policies and experiences', Montevideo: UNESCO. Accessible at: http://unesdoc.unesco.org/images/0024/002460/246055E.pdf.

Sebastian, M. Pak Court Holds Suspension Of Mobile Services By Federal Govt On Ground Of National Security Illegal. Live Law. Accessible at: http://www.livelaw.in/pak-court-holds-suspension-mobile-services-federal-govt-ground-national-security-illegal-read-judgment/.

State Security Agency. 2015. South Africa National Cybersecurity Policy Framework. Accessible at: https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000.

Tshoose, C.I. 2015. Dynamics of Participation in Local Government: A South African Perspective. African Journal of Public Affairs. Accessible at: https://repository.up.ac.za/handle/2263/58158.

UN Human Rights Committee. 1988. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Accessible at: https://www.refworld.org/docid/453883f922.html.

UNHRC. 2013. Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/23/40. Geneva: UNHRC, at para 60. Accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

UNHRC. 2014. Necessary & Proportionate International Principles on the Application of Human Rights to Communications Surveillance. Geneva: UNHRC. Accessible at: https://necessaryandproportionate.org/principles/.

UNESCO. 2014. Fostering Freedom Online: The Role of Internet Intermediaries. Montevideo: UNESCO. 179-180. Accessible at: http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

UNESCO. 2016a. Freedom of Expression and the Internet. Montevideo: UNESCO. Accessible at http://unesdoc.unesco.org/images/0024/002466/246670e.pdf.

UNESCO. 2016b.The Promotion, Protection and Enjoyment of Human Rights on the Internet. Montevideo: UNESCO. 32/13 Accessible at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Pages/ResDecStat.aspx.

UNESCO. 2018. Defining Internet Universality Indicators. Second Draft. Paris: UNESCO. Accessible at: https://en.unesco.org/sites/default/files/unesco_Internet_universality_indicators_second_version.pdf.

UNHRC. 2017. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

University of Minnesota. 1996. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, U.N. Doc. E/CN.4/1996/39. Minnesota: University of Minnesota. Accessible at: http://hrlibrary.umn.edu/instree/johannesburg.html.

Unwanted Witness. 2017. Court Adjourns Social Media Shutdown Lawsuit. Accessible at: https://unwantedwitness.or.ug/court-adjourns-social-media-shutdown-lawsuit/.

APPENDIX 1 ICT POLICY CHECKLIST

OBJECTIVES OF APPENDIX 1

In order to assist policy makers and other stakeholders in the formulation and implementation of ICT policies, set out below is a proposed checklist that addresses the four steps in the ICT policy making process:

- Agenda setting
- Formulation and adoption
- Implementation
- Evaluation and termination.

ICT POLICY CHECKLIST		
No.	**Action**	**Completion**
(i) Agenda setting		
1.	Challenges have been identified through scoping or mapping projects	Yes/no
2.	Stakeholders (including the public and private sector actors) and technical experts have been consulted	Yes/no
3.	Unintended consequences have been identified and considered	Yes/no
(ii) Formulation and adoption		
4.	Extensive public participation processes have been conducted and concluded, and submissions are published openly and considered	Yes/no
5.	Domestic and local contexts have been considered	Yes/no
6.	Policy is drafted in plain language and avoids uncertainty and ambiguity	Yes/no
7.	The policy title and policy statement are simple and to the point	Yes/no
8.	ICT terminology has been clearly defined and a glossary of terms explains concepts and acronyms	Yes/no
9.	It is clear to whom the policy applies and who the relevant institutions and agencies are	Yes/no
10.	The intended objectives and outcomes are detailed and realisable	Yes/no
11.	The core content seeks to remedy the challenges identified	Yes/no
12.	Timeframes and modes of evaluation are expressly defined and realisable	Yes/no
13.	Compliance and enforcement mechanisms are identified or established	Yes/no
14.	Related laws, regulations, and procedures are documented and their harmonisation and alignment has been considered	Yes/no

(iii) Implementation		
15.	Skills development programmes have been established and technical expertise is available	Yes/no
16.	Institutional separation is present and coordination and communications mechanisms have been established	Yes/no
17.	Additional guidelines, frameworks, implementation plans, and technical specifications have been formulated or are in the process of being formulated	Yes/no
18.	Public awareness programmes, training, and education has been incorporated	Yes/no
19.	Compliance is actively measured and documented	Yes/no
(iv) Evaluation and termination		
20.	Structures have been established to collect accurate and reliable data	Yes/no
21.	Appropriate monitoring and evaluating systems have been established	Yes/no

APPENDIX 2 USING THE HANDBOOK AS A TRAINING RESOURCE

OBJECTIVES OF APPENDIX 2

This appendix sets out various tools and exercises to support users in self-driven or guided learning to apply the theory and concepts discussed in this handbook to real-world ICT policy making problems. It prompts discussion on various policy issues explored through this handbook, and includes a quiz to test users' knowledge.

A note for users and trainers

This handbook is intended for all stakeholders involved in the development, implementation, oversight and evaluation of ICT laws and policies. It serves both as a resource in itself, as well as a training manual that can be used by trainers to conduct training workshops for capacity-building.

For any training being conducted, it is strongly recommended that the trainer gauge the level of experience and expertise from the participants beforehand, to ensure that the training being conducted is appropriately rendered. This can be done, for instance, by circulating a questionnaire to the participants before the training.

Set out below are five exercises that can be used, both for self-assessment and for training workshops, as appropriate:

1. The **mapping exercise** is intended to facilitate a scoping of the existing and proposed ICT laws and policies in the user's country, and to understand the opportunities and challenges that these present.
2. The **application of the ICT policy checklist** (Appendix 1) is intended to provide an opportunity to use the proposed checklist in practice, and to develop the checklist to fit the local context.
3. The **discussion questions** are intended to facilitate debate on certain key topical issues that arise in the context of ICT laws and policies.
4. The **drafting scenarios** are intended to give users an opportunity to practise the relevant skills of critically analysing a provision in a law, and undertaking a rights-based assessment of the proposed provision to determine whether it complies with domestic and international law standards.
5. The **quiz** covers content from all four chapters, and is intended to give a snapshot overview of the chapters and the content under consideration. The answers to the quiz questions are contained at the end.

While these exercises are intended to assist in facilitating a better understanding of this handbook – both theoretically and practically – it should be noted that all users and trainers should feel at liberty to use this handbook as they see fit, and develop their own practical exercises and training models that are best suited to their own local context.

1 . Mapping exercise

It is important to understand the ICT regulatory landscape in any country. This helps to identify the objectives, priorities and stakeholders, and to understand how different laws and policies fit together to create the overall framework.

For this exercise, identify the existing and proposed ICT laws and policies in your country. This can include anything that relates to access to ICTs or the exercise of rights online. For example, this might include a law or policy relating to the country's national broadband strategy, cybersecurity, data protection or online content regulation.

Once this has been done, show the relationship between the ICT laws and policies and the relevant stakeholders graphically. This can be done, for example, using a diagram that shows the key ICT legislation in place, the policies that have been formulated or proposed in terms of that legislation, and which government ministry or other state entities have responsibilities in terms thereof.

2. Application of the ICT policy checklist

Identify an ICT policy that has been adopted in your country. Apply the ICT policy checklist to the policy that has been identified, across all four steps as relevant. To what extent have the policy makers in your country met the proposed requirements set out in the ICT policy checklist?

Once this has been done, consider what other relevant considerations should be included in the ICT policy checklist that would be pertinent in your local context, and how the ICT policy checklist can be adapted to better address the domestic needs in your country.

3. Discussion questions

As indicated above, these discussion questions hone in on some of the complex issues that are dealt with in ICT laws and policies, in particular regarding online content regulation. Trainers may approach this in different ways. Trainers should encourage participants to consider and debate opposing viewpoints, to understand the different sides of the argument. Trainers should also encourage participants to undertake independent research to better inform their positions on these topics.

- **Intermediary liability**. As discussed above, different countries have adopted different regulatory approaches to intermediary liability. Discuss the approach that has been taken in your country, and your views on the preferred model proposed by ARTICLE 19.
- **Criminal defamation online**. Various countries across Africa have taken steps to decriminalise defamation, including Kenya, Zimbabwe and Lesotho. However, in South Africa, in *Motsepe v S*,[1] the High Court of South Africa concluded that: "In my view, having regard to the above-mentioned, prosecution of the media journalists who committed a crime of defamation is not inconsistent with the Constitution. In exercising their rights under section 16 of the Constitution, the media should also guard against rights of others as freedom of expression is not unlimited. It must be construed in the context of other rights such as the right to human dignity." Discuss the approach to criminal defamation that has been taken in your country, and what sanctions can be imposed if found guilty. In your view, does this constitute a justifiable limitation – in accordance with the three-part test – of the right to freedom of expression?

[1] Accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2014/1016.html.

- **Internet shutdowns**. In 2015, the mandate holders on the right to freedom of expression, including the UN Special Rapporteur on Freedom of Opinion and Expression and the African Commission of Human and People's Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, published the Joint Declaration on Freedom of Expression and Responses to Conflict Situations.[2] At paragraph 4(c), it is stated that: "Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law." Do you agree with this statement? Discuss what rights are affected by an Internet shutdown, whether there are any circumstances under which an Internet shutdown might be justifiable under human rights law. An additional resource that may be considered to inform your discussion is: Access Now, 'Primer on Internet shutdowns and the law', November 2016.[3]

4.Drafting scenarios

Public participation and engagement on ICT laws and policies are essential to ensuring that the legal instrument under consideration benefits from different expertise, and is truly representative of and responsive to the needs of the public. Set out below are hypothetical examples of ICT laws or policies. Assume that these have been published for comment, and you have been asked to prepare a brief submission on this. Take into account all relevant considerations, including: (i) what is the objective that the provision aims to achieve; (ii) what rights are implicated – either promoted or limited – through this provision; (iii) in the case of a limitation, does the limitation comply with the three-part test for a justifiable limitation; and (iv) does the provision meet its objective. Additionally, indicate what your proposal in relation to the provision would be, such as a complete scrapping of the law or a proposed re-drafting of the wording.

- **False information**. "Any person who, with ill intent, publishes or re-publishes false or misleading information online that has the potential to cause harm in any form, including economic or reputational harm, is guilty of an offence and liable on conviction to imprisonment for up to five years or a fine not exceeding $5 000 (USD) or both."
- **Cybercrimes**. "No person is permitted to wilfully publish any communication online that is either directly or indirectly targeted towards a member of the public, in circumstances where the person responsible for the publication knows or ought to know that such is likely to cause distress, apprehension or fear of violence."
- **Prohibited speech**. "Any person who publishes a statement online that is intended to ridicule, bring into contempt or incite hatred towards any public official is guilty of an offence."

[2] Accessible at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E.

[3] Accessible at: https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Expression/Telecommunications/AccessPart_I.docx&action=default&DefaultItemOpen=1.

5. Quiz

1. Which of the following is a legal instrument that has binding legal effect?
   a. Policy
   b. Legislation
   c. White Paper
   d. Guidelines

2. What fundamental rights can ICT policies facilitate?
   a. Freedom of expression
   b. Access to information
   c. All of the above
   d. None of the above

3. What does the digital divide refer to?
   a. Unequal access to ICTs
   b. Computational analysis
   c. The difference between mobile and fixed line access to the Internet
   d. None of the above

4. What does UN SDG 9 provide?
   a. No poverty
   b. Good health and well-being
   c. Industry, innovation and infrastructure
   d. Peace, justice and strong institutions

5. What does the Human Rights Committee indicate, through General Comment No. 34 on article 19 of the ICCPR, is not compatible with article 19(3)?
   a. Relying on national security as a ground to suppress information from the public of legitimate public interest that does not harm national security
   b. Relying on national security as a ground to withhold information from the public of legitimate public interest that does not harm national security
   c. Relying on national security to prosecute persons, such as journalists or human rights defenders, for having disseminated such information
   d. All of the above

6. What is the general rule on disclosure provided in the Johannesburg Principles?
   a. Disclosure should always be prohibited where national security considerations arise
   b. Members of the public should be given a harsh penalty if any information regarding national security is disclosed
   c. No person should be punished on national security grounds for disclosure of information if the disclosure does not harm a national security interest or the public interest in knowing the information outweighs the harm from disclosure
   d. There is never a justifiable public interest basis for the disclosure of information where national security considerations arise

7. Which of the following is a core element of the right contained in article 19 of the ICCPR?
   a. The right to hold opinions without interference (freedom of opinion)
   b. The right to seek and receive information (access to information)
   c. The right to impart information (freedom of expression)
   d. All of the above

8. What does the Human Rights Committee indicate, through General Comment No. 34 on article 19 of the ICCPR, in respect of the limitation of the rights?
   a. Restrictions on the right must not put the right itself in jeopardy
   b. The interest being protected is irrelevant in the limitations analysis
   c. The right to freedom of expression can never be limited
   d. The right to freedom of expression can only be limited if there is a competing national security consideration

9. Which of the following statements is true?
   a. The UN and the ACHPR have affirmed that the same rights that people have offline must also be protected online
   b. The UN and the ACHPR have indicated that human rights protections do not extend to the exercise of rights online
   c. The UN has affirmed that the same rights that people have offline must also be protected online, but the ACHPR has disagreed with this position
   d. The UN and the ACHPR have yet to consider the application of fundamental rights online

10. What is the relationship between content and applications providers and final consumers?
    a. A final consumer purchasing technical equipment
    b. A network operator purchasing network elements from a network element provider
    c. A final consumer making use of an online service, such as a search engine
    d. The provision of fixed voice, mobile and Internet access services to customers

11. Which of the following is an example of a government stakeholder relevant to the Internet and ICTs?
    a. Commercial Internet service provider
    b. Department of Telecommunications
    c. Organised groups of Internet users
    d. Local non-governmental organisations (NGOs) that advocate for free speech

12. Which of the following is an impediment to regulatory effectiveness?
    a. Political interference in the running of the regulator
    b. Inadequate consultation mechanisms for the involvement of external parties in processes
    c. Lack of consistency in decision making
    d. All of the above

13. Which of the following is responsible for the maintenance of the IP address systems and the management of top level domains?
    a. International Telecommunication Union (ITU)
    b. Internet Corporation for Assigned Names and Numbers (ICANN)
    c. African Network Information Centre (AfriNIC)
    d. Internet Engineering Task Force (IETF)

14. What does the strict liability model of intermediary liability refer to?
    a. Internet intermediaries are liable for third party content, and intermediaries are effectively required to monitor content in order to comply with the law
    b. Internet intermediaries are granted immunity, provided that they comply with certain requirements
    c. Internet intermediaries are granted broad or conditional immunity from third-party content, and exempted from any general requirement to monitor content
    d. All of the above

15. Which of the following is contained in the Manila Principles on Intermediary Liability?
    a. Intermediaries should be shielded from liability for third party content
    b. Content should not be required to be restricted without an order by a judicial authority
    c. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality
    d. All of the above

16. What does the principle of technological neutrality relate to in the development of an ICT policy?
    a. Open access for multiple service providers should be provided, including through a commitment to open governance and open data
    b. Infrastructure sharing should be provided for to avoid unnecessary duplication
    c. No preference should be given to any specific type of service or technology, while ensuring the use of common standards and protocols that enable inter-operability
    d. Conditions for innovation should be created throughout the ICT ecosystem

17. UNESCO had identified four keystones for an open, global and secure Internet. Which of the four keystones do the components of universal access, freedom of information and open knowledge resources relate?
    a. Access to information and knowledge
    b. Freedom of expression
    c. Privacy
    d. Ethics

18. Which of the following statements is true?
    a. The African Declaration on Internet Rights and Freedoms is a binding treaty on all African states regarding freedom of expression
    b. The African Declaration on Internet Rights and Freedoms is a domestic law implemented in all West African states regarding access to information
    c. The African Declaration on Internet Rights and Freedoms is a Pan-African, civil society led initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation
    d. The African Declaration on Internet Rights and Freedoms is a global standard applied and implemented by the United Nations that establishes a global court for Internet-related offences

19. What are the basic technical requirements that a user needs to access the Internet?
    a. Equipment; access to an Internet service provider; a profile picture
    b. Equipment; Internet access software; connectivity; access to an Internet service provider
    c. Equipment; Internet access software; access to an Internet service provider; e-mail address
    d. Internet access software; access to an Internet service provider; social media profile

20. What are the four I's identified by the Broadband Commission for Sustainable Development to expand access to broadband services?
    a. Infrastructure; investment; innovation; inclusivity
    b. Infrastructure; investment; intelligence; inclination
    c. IT skills; implementation; innovation; inclusivity
    d. Infrastructure; isolation; international growth; inclusivity

21. What did the 2011 Joint Declaration on Freedom of Expression and Internet state regarding the blocking and filtering of content?
    a. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses is an extreme measure that can only be justified in accordance with international standards
    b. Content filtering systems that are imposed by a government or commercial service provider, and that are not end-user controlled, are a form of prior censorship and are not justifiable as a restriction on freedom of expression
    c. Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering
    d. All of the above

22. What does the Excise Duty (Amendment) Act, 2018 passed by the Ugandan Parliament provide?
    a. All bloggers must apply for a licence before being permitted to post online
    b. A telecommunication service operator providing data used for accessing over-the-top (OTT) services is liable to account for and pay excise duty on such access
    c. Members of the public must obtain a licence before being permitted to post any video on the Internet
    d. All of the above

23. What did the High Court of Zimbabwe rule in the matter instituted by Zimbabwe Lawyers for Human Rights and the Media Institute of Southern Africa: Zimbabwe Chapter against the government of Zimbabwe regarding the Internet shutdown in January 2019?
    a. That the Interception of Communications Act was unconstitutional
    b. That the President of Zimbabwe is empowered under domestic and international law to cause an intentional network disruption, provided that it is for national security reasons
    c. That the Minister of State in the President's Office for National Security was not assigned with any authority to issue the directive to cause the network disruption
    d. That the matter was not urgent, and therefore stood to be dismissed

24. One of the key principles of data protection is purpose specification. What does this relate to?
    a. Personal data must be collected only for specified, explicit, and legitimate purposes
    b. Data collectors should be open about the data that is being collected
    c. Data subjects must be provided with a right of access to the data collected about them
    d. Personal data should be protected by reasonable security safeguards

- There are four steps in the ICT policy making process: Agenda setting → Formulation and adoption → Implementation → Evaluation and termination. Which of the following statements is false?
    e. ICT policy formulation should be a broad and extensive consultative process which should be developed through a series of stakeholder engagements
    f. Public participation is irrelevant to the ICT policy making process
    g. An ICT policy needs to be monitored and evaluated throughout the course of implementation
    h. Evaluation is often based on data and various types of analysis

25. Which of the following measures is used in the ITU Digitisation Index?
    a. Affordability; infrastructure reliability; network access; capacity; usage; human capital
    b. Rights; openness; accessibility to all; multi-stakeholder; cross-cutting
    c. Freedom of expression; access to information; privacy
    d. None of the above

26. ICT policies should be drafted in plain language. What does this mean?
    a. ICT policies must inevitably use technical jargon
    b. ICT policies should be targeted towards people with technical expertise
    c. ICT policies should be drafted in precise and short sentences, in simple language that is accessible to a broader public audience
    d. ICT policies should not contain a section with definitions

27. In respect of the implementation of ICT policy, which of the following statements is false?
    a. Effective ICT polices often establish or delegate implementation authority to institutions other than those that drafted the policy
    b. In order to ensure effective implementation, a series of technical documents should be formulated and drafted, alongside the ICT policy
    c. ICT policies are typically implemented by one government department in isolation from other state departments
    d. Enforcement or oversight mechanisms are necessary to ensure citizen-led accountability in the implementation process

APPENDIX 2

Answers to quiz

1	b
2	c
3	a
4	c
5	d
6	c
7	d
8	a
9	a
10	c
11	b
12	d
13	b
14	a

15	d
16	c
17	a
18	c
19	b
20	a
21	d
22	b
23	c
24	a
25	b
26	a
27	c
28	c

APPENDIX 3 RECOMMENDED RESOURCES

OBJECTIVES OF APPENDIX 3
This appendix is a list of recommended resources that can be used either for more information, or in the structuring of a training session or programme.

1. Association for Progressive Communications, 'The APC ICT policy handbook', 2009: https://www.apc.org/sites/default/files/APCHandbookWeb_EN_0.pdf.

2. Broadband Commission for Sustainable Development, 'The state of broadband: Broadband catalyzing sustainable development', 2018: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.19-2018-PDF-E.pdf.

3. Centre for Intellectual Property and Information Technology Law, 'Africa ICT policy database', 2018: https://www.ictpolicy.org/about#/details/1.

4. eTransform Africa, 'ICT competitiveness in Africa', 2015: https://openknowledge.worldbank.org/handle/10986/19025.

5. Global Partners Digital, 'Travel guide to the digital world: Internet policy and governance for human rights defenders', 2014: https://www.gp-digital.org/wp-content/uploads/2014/06/Travel-Guide-to-the-Digital-Worlds-1.pdf.

6. Global Partners Digital, 'Framework for multi-stakeholder cyber policy development', 2018: https://www.gp-digital.org/publication/multistakeholder-framework/.

7. ITU, 'Regulatory challenges and opportunities in the new ICT ecosystem', 2018: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT03-2018-PDF-E.pdf.

8. ITU, 'The economic contribution of broadband, digitization and ICT regulation', 2018: https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/FINAL_1d_18-00513_Broadband-and-Digital-Transformation-E.pdf.

9. Media Legal Defence Initiative, 'Training manual on digital rights and freedom of expression online', 2018: https://www.mediadefence.org/resources/mldi-training-manual-on-digital-rights-and-freedom-of-expression-online/.

10. Research ICT Africa, 'ICT4D, regulation and strategy', 2015: https://researchictafrica.net/publications/Other_publications/2015_Gillwald_-_ICT4D_Regulation_and_strategy.pdf.

11. UNESCO, 'Freedom of expression and the Internet', 2016: http://unesdoc.unesco.org/images/0024/002466/246670e.pdf.

12. UNESCO, 'Internet universality indicators: A framework for assessing Internet development', 2018: http://unesdoc.unesco.org/images/0026/002658/265830e.pdf.