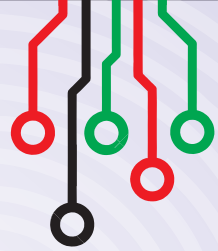




**MZALENDO**



# **DIGITAL RIGHTS IN** **KENYA REPORT**

Published by  
**MZALENDO TRUST**  
P. O. Box 21765 - 00505  
Nairobi, Kenya  
Email: [info@mzalendo.com](mailto:info@mzalendo.com)  
Website: [www.mzalendo.com](http://www.mzalendo.com)

This work was carried out in the Context of the African Digital Rights Fund with support from the collaboration on ICT Policy for East And Southern Africa (CIPESA)

---

© Copyright Mzalendo Trust, 2019

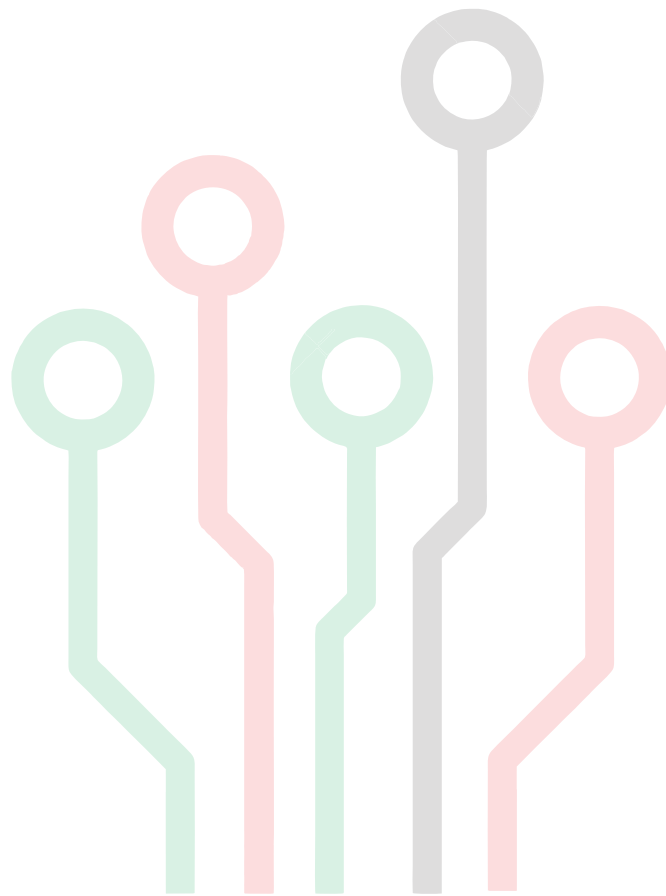
---

All rights reserved. No part of this report may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopy, recording or by any information storage and retrieval system without permission in writing from the publisher except in the case of brief questions embodied in critical reviews and articles and for educational purposes.

---

Design, Layout & Printing  
Blue Graphics Limited.

# MZALENDO TRUST



## DIGITAL RIGHTS IN KENYA REPORT

---

E-mail: [otele@uonbi.ac.ke](mailto:otele@uonbi.ac.ke); [otelemeywa@yahoo.com](mailto:otelemeywa@yahoo.com)

Telephone: 0729276892

# TABLE OF CONTENT

LIST OF FIGURES .....	v
<b>CHAPTER ONE: INTRODUCTION</b> .....	<b>1</b>
1.1 Study Background and Problem Statement .....	1
1.2 Objectives of the Study .....	2
1.3 Study Methodology .....	2
1.4 The structure of the report .....	2
<b>CHAPTER TWO: HISTORICAL REVIEW OF DIGITAL RIGHTS AND ACCOMPANYING LAWS</b> .....	<b>3</b>
2.1 Pre-Independence Era .....	3
2.2 Post-Independence Era .....	3
2.2.1 From 1963-2010 .....	3
2.2.2 From 2010 to Date5 .....	5
<b>CHAPTER THREE: THE LEGAL FRAMEWORK ON THE RIGHTS TO ACCESS TO INFORMATION AND DIGITAL RIGHTS IN KENYA</b> .....	<b>7</b>
3.1 The Constitution of the Republic of Kenya, 2010 .....	7
3.2 Access to Information Act No 31 of 2016 .....	8
3.3 The Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 .....	10
3.4 The Computer Misuse and Cybercrimes Act No. 5 of 2018 .....	10
3.3 The Data Protection Act No. 24 of 2019 .....	10
3.4 The Proposed Huduma Bill, 2019 .....	10
3.5 The Data Protection Act No. 24 of 2019 .....	11
3.6 The Proposed Huduma Bill, 2019 .....	12
<b>CHAPTER FOUR: ANALYSIS OF RECENT HUDUMA JUDGEMENT</b> .....	<b>14</b>
4.1 The Registration Process Infringed on the Rights to Privacy .....	14
4.2 Kenya Lacks a Comprehensive Data Protection Law .....	15
4.3 The Registration Process Lacked Legal Basis .....	16
4.4 The Process Would Marginalize Persons who have not Acquired the Primary Documents Required to Register for Huduma Namba .....	16
<b>CHAPTER FIVE: PERCEPTIONS, IMPLEMENTATION AND IMPACT OF THE RELEVANT LEGISLATION AND POLICY PROPOSALS</b> .....	<b>18</b>
5.1 Right to Access to Information .....	18
5.2 Right to Privacy .....	21
5.3 NIIMs and associated Huduma Namba and Card .....	26
<b>CHAPTER SIX: POTENTIAL OPPORTUNITIES FOR ENHANCING AND ADVANCING DIGITAL RIGHTS IN KENYA</b> .....	<b>31</b>
6.1 Technology Spread and Increased Adoption of ICT in Work and Social Places .....	31
6.2 Increased Participation of Private Entities .....	32
6.3 Litigation of Digital Rights .....	32
6.4 Advocacy Work .....	32
6.5 Digital Safety and Digital Literacy .....	32
6.6 Regulatory Framework .....	32
6.7 Increased Government Support .....	32
<b>CHAPTER SEVEN: CONCLUSION</b> .....	<b>33</b>
7.1 Summary .....	33
7.2 Emerging Issues .....	34
<b>REFERENCES</b> .....	<b>36</b>



# LIST OF FIGURES

<b>Figure 1:</b> Satisfaction Level with the Implementation of Article 35	19
<b>Figure 2:</b> Familiarity with the existence of Access to Information Act, 2016	19
<b>Figure 3:</b> Extent of the implementation of the right to information access since the enactment of the Act	20
<b>Figure 4:</b> Impact of the Implementation of Access to Information Act, 2016	20
<b>Figure 5:</b> Suggestions of the review of the Act	21
<b>Figure 6:</b> Satisfaction with the implementation of Article 31 of the Constitution	22
<b>Figure 7:</b> Familiarity with the existence of Data Protection Act, 2019	23
<b>Figure 8:</b> Familiarity with existence of Computer Misuse and Cybercrimes Act, 2018	23
<b>Figure 9:</b> Satisfaction level with regard to the Implementation of the Data Protection Act, 2019	24
<b>Figure 10:</b> Satisfaction level with the Implementation of Computer Misuse and Cybercrime Act, 2018	24
<b>Figure 11:</b> Impacts of Computer Misuse and Cybercrimes Act, 2018 and the Data Protection Act 2019	25
<b>Figure 12:</b> Suggestions on regulation to enhance the right to privacy	26
<b>Figure 13:</b> Accuracy of data in the NIIMs	27
<b>Figure 14:</b> Data controls in the NIIMs	27
<b>Figure 15:</b> Security of data in the NIIMS	28
<b>Figure 16:</b> Extent of lawfully, transparency and fairness in the utilization of data in the NIIMs	28
<b>Figure 17:</b> Implementation cost and sustainability of the NIIMs	29
<b>Figure 18:</b> Proposed mandatory uses of Huduma Namba and Card when transacting with government	29

# LIST OF ABBREVIATIONS

<b>ADRF</b>	Africa Digital Rights Fund
<b>BAKE</b>	Bloggers Association of Kenya
<b>CA</b>	Communications Authority of Kenya
<b>CIPESA</b>	Collaboration on International ICT Policy for East and Southern Africa
<b>CCK</b>	Communication Commission of Kenya
<b>COK</b>	Constitution of Kenya
<b>CORD</b>	Coalition for Reform and Democracy
<b>DNA</b>	Deoxyribonucleic Acid
<b>GDP</b>	Gross Domestic Product
<b>GDPR</b>	General Data Protection Regulation
<b>GPS</b>	Global Positioning System
<b>ICT</b>	Information, Communication & Technology
<b>KBC</b>	Kenya Broadcasting Corporation
<b>NDRS</b>	National Digital Registry System
<b>NIIMS</b>	National Integrated Identity Management System
<b>OECD</b>	Organization for Economic Co-operation and Development



# FOREWORD AND ACKNOWLEDGEMENTS

---

Article 31 of the Constitution of Kenya 2010 provides for the right to privacy. The importance of this right is to ensure the protection of citizens' personal data and to protect against undue revelation of information relating to family or private affairs of an individual. Further, the right to access information is also guaranteed under Article 35 and allows access to information held by the State and aids in promotion of good governance through openness, transparency and accountability.

Data security and access to information are increasingly assuming a very critical place in political, economic and social governance. With most transactions shifting to the online space, whether banking, shopping or defraying of expenses, there is increasing need to ensure protection of personal data as collected by either the State or private entities. The adoption of the General Data Protection Regulation (GDPR) by the European Union signalled a new era in data protection. In 2019, the National Assembly of Kenya enacted the Data Protection Act that provides for the regulation of processing of personal data. To secure access to information rights, the National Assembly passed the Access to Information Act in 2016.

In light of this, Mzalendo Trust commissioned this study with a view of broadly informing public's appreciation of the actual implementation of the digital rights and access to information legal regimes. It sought to achieve this by specifically reviewing Kenya's digital rights historical developments; reviewing the existing digital rights and access to information legal regime; analyzing the Huduma Namba judgement; gauging public's appreciation of the implementation of the existing legal regimes; identification of challenges facing the enhancement of digital rights and the potential opportunities. Importantly, the study is situated within the context of the COVID-19 pandemic, and the implications of the pandemic on digital rights and access to information. The study is intended to creatively and constructively inform the evolving digital rights and access to information discourse. It aims to boost civic awareness on digital rights and access to information and to increase civic engagement in improving corresponding regulation.

Mzalendo Trust is greatly indebted to the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) who, through the Africa Digital Rights Fund (ADRF), offered financial and technical support that enabled the organization to successfully carry out and publish the findings of this study.

I wish to thank everyone involved in generating this publication, in particular, all the respondents who provided immense contributions and recommendations, including the Ministry of Information, Communications and Telecommunication, the Ministry of Interior and Coordination of the National Government, the Judiciary, mobile phone service providers, digital rights experts, civil society actors, academia, the media and all the participants at the validation meeting held prior to launch of this Report. I also express utmost gratitude to the Consultant, Dr. Oscar Meywa Otele as well the staff at Mzalendo Trust, Alex Ogutu, Loise Mwakamba, Jefferson Gathumbi and Sylvia Katua for excellent work and valuable technical direction.

**Ms. Caroline Gaita,  
Executive Director  
Mzalendo Trust.**

# EXECUTIVE SUMMARY

---

This study sets to understand digital rights in Kenya. It reviews the history regarding digital rights and accompanying laws in Kenya; and reviews existing data rights and access to information laws in Kenya, and their implementation. In addition, it analyzes the Huduma Namba judgement and identifies the perceptions of the impact of the implementation of the relevant legislation and regulations. It concludes by identifying potential opportunities for enhancing and advancing digital rights in Kenya.

Methodologically, the study is anchored on both primary and secondary data. The former was obtained through structured questionnaires completed by purposively selected respondents drawn from academia, civil society and relevant government agencies. Secondary data was derived through documentary analysis. The Report highlights that from colonialism to independence to post-independence era, the growth and development of digital rights and accompanying laws have taken different shades involving a complex set of organizations, actors and institutions.

Despite the evolving legal framework on digital rights, the regulatory framework is yet to fully develop thereby potentially threatening the implementation of the rights to access information and digital rights. The study is optimistic that the following opportunities can promote digital rights in Kenya: technology spread and increased adoption of ICT in work and social places; increased participation of private entities; litigation on digital rights; advocacy work; digital safety and digital literacy and increased government support.



# CHAPTER ONE

---

## INTRODUCTION

### 1.1 Study Background and Problem Statement

Recently, a majority of African states have embarked on digital transformation and promotion of digital economy (Thiel 2020, p.115). According to the World Bank (2018), approximately 496 million Africans are excluded from accessing state services because of lack of official documentation of their legal personhood. In light of this problem, utilizing modern technologies, African governments are now making efforts to collect personal data hailed as a potential solution to the deeply rooted issue of incomplete state recognition system (Gelb & Clark 2013). With this increasing effort at digitization, there have been concerns over data protection in most African states.

Kenya has experienced growth in technology impacting the way data is generated, processed, stored and accessed. Kenya's National ICT policy acknowledges the importance of accessing information and safeguarding it. The ever growing computing and communicating technologies are collecting and transmitting data. However, challenges with access to information and the unregulated and arbitrary use of personal data is increasingly becoming a critical area that requires to be managed carefully.

Access to information and digital rights gained momentum following the promulgation of the Constitution of Kenya, 2010 (COK, 2010), with the centrality of each gaining unprecedented public attention following the enactment of respective statute laws. The enactment of the Access to Information Act, 2016, the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 and later Data Protection Act, 2019 were thought as likely to safeguard the right to access information and privacy. Among other things, the Statute Law (Miscellaneous Amendment) Act, 2018 established the National Integrated Identity Management System (NIIMS) intended to be the only source of personal information of all Kenyans as well as foreigners resident in Kenya. A section of the public raised concern and filed a suit at the High Court, expressing strong reservations on the security of their data<sup>1</sup>.

As the court considered counter-arguments, the Data Protection Act No. 24 of 2019 was enacted aimed at enforcing privacy rights. Despite this, there is no clear implementation and regulatory frameworks for the

---

<sup>1</sup>Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR

realization of these privacy rights. What is more, there is lack of implementation of other related legislation such as the Access to Information Act, 2016, yet Kenyans continue to interact and transact via online space. It is against this background that there is need to assess the current legal framework, gauge perceptions about implementation and how digital rights in Kenya could be improved.

## 1.2 Objectives of the Study

More specifically, the study sought to:

- Review the history regarding digital rights and accompanying laws in Kenya;
- Review existing data rights and access to information laws in Kenya, and their implementation;
- Analyze the recent Huduma Namba judgment and;
- Identify the perceptions of the impact of the implementation of the relevant legislation and regulations and;
- Identify potential opportunities for enhancing and advancing digital rights in Kenya.

## 1.3 Study Methodology

The study combined quantitative and qualitative research methodologies. A combination of methodologies allowed for complementarity in the weaknesses identified in one approach. Both secondary and primary data were collected. Secondary data was obtained from existing relevant academic literature with a view of understanding how access to information and privacy rights are safeguarded in other jurisdictions. Primary data was collected at two levels. At the first level, the study reviewed legal framework governing access to information and protection of personal data. At the second level, the researcher collected data from key informants using a questionnaire generated by survey monkey via WhatsApp platform. Further follow-up was made through phone calls and email communication for clarification of some of the emerging issues.

## 1.4 The structure of the report

This Report is organized into six chapters. The introductory chapter outlines the study background and problem statement; study objectives and the study methodology. Chapter Two presents historical review of digital rights and accompanying laws. Chapter Three highlights legal framework underpinning the right to access information and privacy, while Chapter Four analyzes Huduma Namba judgment. Chapter Five presents perceptions about the implementation of digital rights in Kenya. Chapter Six highlights opportunities for enhancing digital rights in Kenya, with conclusion as the last Chapter.



# CHAPTER TWO

## HISTORICAL REVIEW OF DIGITAL RIGHTS AND ACCOMPANYING LAWS

*This chapter presents a historical review of digital rights and accompanying laws in Kenya.*

### 2.1 Pre-Independence Era

Understood as “human rights in the digital era and in the access and use of the internet and other ICT”<sup>2</sup>, digital rights and their development in Kenya are traceable to colonial era. As a strategy to control freedom of movement and association, the colonial authority enacted the Native Registration Ordinance of 1915 which introduced the Kipande System that registered a fingerprint or single thumb of the applicant. The registration ordinance was amended in 1949 as to make provision for the registration of persons and for the issue of identity cards. Section 2 of the Act applied to all Kenyan citizens aged 18 years and above or where there was no evidence of age, it was apparent that the applicant was 18 years and above. Although the registration requirement extended fingerprinting to everybody in the colony, the system restricted the name and location of the applicants (Breckenridge 2019, p.95). Following the emergency of Mau Mau Movement in 1952 the fingerprinting system was upgraded to full-print capture and two years later the colonial authority imposed on all adult “members of the Kikuyu and allied tribes” compulsory booklet requiring ten fingerprints stored that registered official authority for movements and settlement. However due to inadequate resources the colonial authority was unable to sustain ten-print registration after the emergency (Breckenridge 2019, p.95).

### 2.2 Post-Independence Era

#### 2.2.1 From 1963-2010

At independence in <sup>1963</sup>, the Constitution provided an elaborate Bill of Rights modeled along the lines of the European Convention on Human Rights. Section <sup>79</sup> of the Constitution allowed every person to enjoy the freedom to “hold information as well as receive ideas and information without inferences from the state or any agencies<sup>3</sup>. Though this was not absolute, as it was limited on the basis of national security, safety and

<sup>2</sup>Sarah Nyakio “Digital rights; the Present and the Future”, ICJ-Kenya, <https://www.icj-kenya.org> (Accessed 24 April 2020).

<sup>3</sup>Section 79(1) of the Constitution of Kenya.

<sup>4</sup>Section 79(2) of the Constitution of Kenya.

public health<sup>4</sup>. The Constitution also provided for clear provisions on citizenship. Every adult citizen aged 18 years and above was entitled to national identification card, but it was not until 1979 that the government legally specified ten-print registration through the amendment to the Registration of Persons Act. This form of acquiring national identification document went on until 1995 before the shift to the new generation smaller identity card.

During this period, there were numerous pieces of legislation that were enacted to reinforce the right of access to information. These legislations governed information transmitted through print and electronic platforms. For example, Kenya Broadcasting Corporation (KBC) established by the Kenya Broadcasting Corporation Act (1998) which regulated the production and broadcasting of programmes by sound or television<sup>5</sup>. The Films and Stage Play Act (1998), enacted to regulate the making and exhibition of films and plays, had provisions governing access to information by the public<sup>6</sup>. However access to information by these legislations was limited by other laws, especially on the grounds of national security. For example, Official Secret Act of 1970s limited access to information if, in the view of the State, the information was “calculated to be or might be or [was] intended to be directly or indirectly useful for a foreign power or disaffected person<sup>7</sup>”. Similarly, the 1985 Service Commissions Act and the 1998 National Assembly (Powers and Privileges) Act to a large extent limited the amount of information made available to the public. These laws gave the government a lot of power to limit the circulation of information held by the State. Further, the Preservation of Public Security Act gave the President a lot of powers to make any regulations limiting communication “of any information<sup>8</sup>” on the basis of national security. The 1985 Penal Code granted the Ministry of Internal Security sweeping powers to limit any importation or production of any publication mainly on national security grounds. Public policy was also cited as another reason for refusal to disclose information. For example, the 1989 Evidence Act gave public officers powers to decide whether to release any information in their possession that could be prejudicial to public policy<sup>9</sup>. With advancement of computers and information technologies toward the end of 20th century, the enactment of Kenya Communication Act No. 2 of 1998 was a key milestone as it provided for data protection that enables timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes.

When Mwai Kibaki ascended to power in December 2002, he radically transformed the access and use of internet and other ICTs. Under the hitherto existing constitutional dispensation the new regime fundamentally widened freedom of expression through media freedom. As part of the liberalization measures, the regime empowered Communication Commission of Kenya (CCK) (now Communications Authority of Kenya-CA) seeing upsurge of media houses between, 2002-2009 (Kivikuru 2017, p.309). Recognizing that information technology was a key driver of economic growth, President Kibaki’s brainchild development policy- Economic Recovery Strategy Paper, 2003-2007 saw concerted partnership between Kenya and external financiers in promoting ICT access in the country. Thus, Kenya Rural Telecommunications Development Project funded by the Chinese government at a cost of US\$21.75 million was instrumental in promoting internet access and connectivity in the country so much that Kenya surpassed Africa’s internet penetration average by almost 50 percent of the population<sup>10</sup>. These advancements were later detailed in the Information and Communication Technology (ICT) Policy of March 2006 which acknowledged the importance of accessing information and safeguarding ICTs.

The launch of Kenya Vision 2030 in June 2008 further provided a policy environment for the development of digital rights. Kenya envisioned herself as “an ICT hub and a globally competitive digital economy” premised on six principles: partnership, equity and non-discrimination, technology neutrality, environmental protection and conservation, good governance and the provision of incentives to local private sectors to provide ICT solutions (Republic of Kenya 2008). Although the long-term vision draws a nexus between technological

<sup>5</sup>Chapter 221 of the Laws of Kenya.

<sup>6</sup>Chapter 222 of the Laws of Kenya.

<sup>7</sup>Section 3(1).

<sup>8</sup>Section 4.

<sup>9</sup>Sections 131-133.

<sup>10</sup><http://www.internetworldstats.com/stats1.htm>(Accessed on 17th March 2020).



development and democracy, it lends itself more on technology while ignoring the utility of ICT in service sectors such as health, agriculture, transport, education and business (Kivikuru 2017, p.313), where a majority of citizens are found. The Kenya Communications Act (No. 2 of 1998) and as amended by the Kenya Communications (Amendment) Act, 2009, provided the main framework for regulating the communications sector in Kenya.

### 2.2.2 From 2010 to Date

The promulgation of 2010 Constitution was yet another milestone in the realization of digital rights and access to information. Articles 31 and 35 provide the constitutional foundation of the right to privacy and access to information respectively. Later in 2013 the Ministry of Information, Communication and Technology reviewed the National ICT policy placing more emphasis on access to information and internet, and in the same year the Ministry launched a strategic plan (2013-2017) hailed as strongly technology oriented. The Ministry emphasized coordination and cooperation in ICT processes between the national government and county governments. Subsequently, President Uhuru Kenyatta launched The Kenya National ICT Masterplan (2014-2018) anchored on three foundations, namely: the significance of human resources as a prerequisite for ICT progress; the integrated ICT infrastructure; the integrated information infrastructure (Masterplan 2014, p.48). In terms of ICT's human capacity, the desired outcomes were the availability of high-quality workforce for business, but also "ICT literate population capable of exploiting ICT products and services for improved quality of life" (Masterplan 2014, p. 48). Although the citizens are included, the shortcoming of the Masterplan is that the strategies to attain the goals are considerably more detailed in terms of the workforce qualification than ICT literacy for the public.

The Masterplan introduced the idea of e-government, seeing it as the driver of Kenya's economy. E-government is described as

leverage[ing] information and communication technology to strengthen and improve the quality and efficiency of public administration. Communication is made easier for citizens and businesses costs are lowered and at the same time international processes are sped up substantially. The quality and transparency of public services is raised considerably to everyone's benefit (cited in Kivikuru 2017, p.313).

In 2014, the government announced plan to develop the National Digital Registry System (NDRS) for "panoptic biometric registration" (Breckenridge 2019, p.92) but failed due to competing interests between banks, donors, telecom firms, politicians and bureaucrats. In recognition that interactions and transactions are increasingly shifting to the online space, the government enacted Computer Misuse and Cybercrimes Act No. of 2018. Section 20 of the Act provides additional protection that enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes. After numerous debates, review and consultations<sup>11</sup>, Access to Information Act was enacted in 2016, giving full effect to Article 35 of COK, 2010 on the right of access to information.

In November 2018, the government revived its original idea of NDRS through the Statute Law (Miscellaneous Amendments) Act No. 18 of 2018. The effect of the Act was to amend several provisions of a number of existing statutes, among them the Registration of Persons Act (Cap 107 of the Laws of Kenya). The amendments to the Act established a National Integrated Identity Management System (NIIMS) whose registration process assigned applicant a number popularly known as Huduma Namba<sup>12</sup>. Recognizing that indeed there existed a policy gap, the Ministry of Information, Communications and Technology, released

<sup>11</sup>In fact the first attempt to draft such legislation began in 2001/2002 by a group of civil society, then second attempt in 2005 and then third attempt in 2007.

<sup>12</sup>Translated as unique number for service delivery.

National Information, Communications and Technology (ICT) Policy in November 2019 with objectives of one, creating the infrastructural conditions that would enable the use of always-on, high speed, wireless, internet across the country. Two, facilitating the creation of infrastructure and frameworks that support the growth of data centres, pervasive instrumentation (Internet of Things), machine learning and local manufacturing while fostering a secure, innovation ecosystem. Three, growing the contribution of ICT to increase the overall size of the digital and traditional economy to 10% of GDP by 2030, by using ICT as a foundation for the creation of a more robust economy, providing secure income and livelihoods to the citizenry. Four, positioning the country to take advantage of emerging trends such as the shared and gig economy, by enhancing our education institutions and the skills of our people and by fostering an innovation and start-up ecosystem that is able to lead in the adoption of emerging trends on a global scale. Five, gaining global recognition for innovation, efficiency and quality in public service delivery. Government services will be delivered in a manner that ensures we have a prosperous, free, open and stable society. Finally, in recognition that there was need to protect personal data, the Data Protection Act was enacted in 2019.



# CHAPTER THREE

## THE LEGAL FRAMEWORK ON THE RIGHT OF ACCESS TO INFORMATION AND DIGITAL RIGHTS IN KENYA

*Drawing from the previous chapter, we note that in Kenya, serious journey towards access to information and protection of personal data began with the promulgation of the COK, 2010, which set out an extensive legal framework on access to information, protection of the integrity of government records and information as well as data protection, information security and modalities. This chapter elaborates relevant sections of the Constitution and the subsequent statute laws.*

### 3.1 The Constitution of the Republic of Kenya, 2010

The Constitution of Kenya, 2010 (COK, 2010) is the ‘supreme law of the Republic (of Kenya), and binds all persons and all State organs at both levels of government ( National and county)<sup>13</sup> . The document lays the foundation for the respect and protection of the fundamental rights and freedoms as stipulated in the Bill of Rights, touted as one of the most progressive and liberal regimes of human rights in the region<sup>14</sup>. These rights, including the right to privacy and right to access to information must be respected, upheld and protected by all organs and agencies of the government as well as individuals<sup>15</sup>. Article 10 of the COK further provides national values and principles of governance such as rule of law, democracy, participation of the people, integrity, transparency and accountability key in the implementation of access to information and privacy right.

Article 31 of the Constitution on the right to privacy states that “(E)very person has the right to privacy, which includes the right not have- (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy

<sup>13</sup> Article 2 (1), of the Constitution of Kenya, 2010, p.14.

<sup>14</sup> Chapter Four of the Constitution is entitled: Bill of Rights.

<sup>15</sup> Ibid Part 2. Other rights provided in the Bill of Rights inter alia include: Right to life; equality and freedom from discrimination; human dignity; freedom and security of the person; slavery, servitude and forced labour; privacy; freedom of conscience, religion, belief and opinion; freedom of expression; freedom of the media; freedom of association; assembly, demonstration, picketing and residence; protection of right to property; labour relations; environment; economic and social rights and language and culture; family; consumer rights, fair administrative action; access to justice; rights of arrested persons; fair hearing and rights of persons detained, held in custody or imprisoned.

of their communications infringed<sup>16</sup>, while Article 35 on the right to access to information provides that: “(1) Every citizen has the right of access to- (a) information held by the State; and (b) information held by another person and required for the exercise or protection of any right or fundamental freedom<sup>17</sup>” .

Evidently, while Article 31 guarantees a general right to privacy, while also guarding against specific infringements of privacy, including unnecessary revelation of information relating to family or private affairs, Article 35 of the Constitution forms the basis for the public right to access to information, as it clearly spells out the rights of a person regarding access information or misleading information relating to the affected person. It also stipulates the responsibility of the State relating to the publication of information that relates to the State. It follows that citizens cannot be denied access to information unless it is proven by the State that the required information falls within the limitations provided under Article 24 of the Constitution. The constitutional limitations could be viewed as guiding parameters against any attempt at violating the rights and freedoms, including the right to privacy and access to information, and must be interpreted and enforced in the context of the article to the extent that the limitation is acceptable and demonstrably justifiable in a free and democratic society<sup>18</sup>. In this context, it means that where a refusal for a claim to privacy and access to information is not ‘acceptable and demonstrably justifiable’, such a refusal is deemed to be in violation of the constitutional rights to privacy and access to information. For access to information, disclosure of such information may be useful in combating corruption and checking on the abuse of power in Kenyan governance. Also, respecting demands to access to information is a critical component in enhancing and promoting the democratic values of transparency and accountability. Article 35 on Access to Information is therefore vital in ensuring that publicly-held information is timeously available to the public in order to enable them to be informed and kept abreast of government decision-making matters and issues that have a direct bearing on the protection of their fundamental rights and freedoms.

Although the right to privacy has received multiple interpretations, the court in *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others* attempted to clarify that it “protects against the unnecessary revelation of information relating to family or private affairs of an individual. Private affairs are those matters whose disclosure will cause mental distress and injury to a person and there is thus need to keep such information confidential. Taken in that context, the right to privacy protects the very core of the personal sphere of an individual and basically envisages the right to live one’s own life with minimum interference. The right also restricts the collection, use of and disclosure of private information<sup>19</sup>”.

Further, although the Constitution stipulates that everyone has the right to demand any information that is in the possession of the State, the broad definition of State that includes two levels of government and their accompanying institutions places greater burden on the State than private bodies. Further, the constitutional interpretation of person includes companies, associations, or other body of persons whether incorporated or unincorporated<sup>20</sup>. It is not clear whether the said person also include private citizens like bloggers whom may be in possession of the information. The Constitution bestows a duty and responsibility on Parliament to enact national legislation giving effect to these rights as discussed below.

### 3.2 Access to Information Act No 31 of 2016

The Act was enacted to give full effect to Article 35 of COK, 2010 on the right of access to information<sup>21</sup>, and empower the Commission on Administrative Justice with oversight and enforcement functions. Read together with Article 10 on national values and principles of governance, the Act seeks to promote good governance through efficient, effective, transparent and accountable government by providing full effect

<sup>16</sup> Article 31 of the Constitution of Kenya, 2010, p. 22.

<sup>17</sup> Article 35 of the Constitution of Kenya, 2010

<sup>18</sup> Article 24 of the Constitution of Kenya, 2010.

<sup>19</sup> *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others*

<sup>20</sup> Article 260 of the Constitution of Kenya.

<sup>21</sup> Article 35 of the Constitution of Kenya, 2010, p. 25.



to the constitutional right to access information. The objects of the Act include, inter alia: to give effect to the right of access to information by citizens as provided under Article 35 of the Constitution; provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information on request in line with the constitutional principles; provide a framework to facilitate access to information held by private bodies in compliance with any right protected by the Constitution and by other law; promote routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency and public participation and access to information; provide for the protection of persons who disclose information of public interest in good faith; and provide a framework to facilitate public education on the right to access information under [the] Act<sup>22</sup>.

According to the Act, a person is entitled to access information if he/she provides reasons<sup>23</sup>. Under Section 14 of the Act, a request for information is deemed to be refused where an applicant fails to receive response from information access officer regarding the requested information within the period contemplated<sup>24</sup>. What is more, the Act guarantees that a person may apply for the review decision from the Commission on Administrative Justice in instances where his/her request for information is refused<sup>25</sup>. Furthermore, the Act safeguards for the protection of the data and provides that it is an offence for any person to disclose exempt information in contravention of the Act. Section 28 of the Act makes provisions for the punishment of three years' imprisonment or a fine not exceeding one million or both to any person who knowingly discloses exempt information, including information that entails unwarranted invasion of the privacy of an individual.

In realizing the above objects, the Act stipulates the right of everyone to information held by the State or private entities by identifying the classes of information to which Article 35 of the Constitution relates. Section 6 (1) of the Act further clarifies the limitations in respect to the right of access to information. It states that such rights shall be limited in respect of information whose disclosure is likely to: undermine the national security of Kenya; impede the due process of law; endanger the safety, health or life of any person; involve the unwarranted invasion of the privacy of an individual, other than application or the person on whose behalf an application has, with proper authority, been made; substantially prejudice the commercial interests, including intellectual property rights, of that entity or third party from whom information was obtained; cause substantial harm to the ability of the Government to manage the economy of Kenya; significantly undermine a public or private entity's ability to give adequate and judicious consideration to a matter concerning which no final decision has been taken and which remains the subject of active consideration; damage a public entity's position in any actual or contemplated legal proceedings; or infringe professional confidentiality as recognized in law or by the rules of a registered association of a profession<sup>26</sup>. This implies that there are circumstances where request to access certain information could be maliciously rejected under the disguise of falling under the limitations. Following this, it could be argued that whereas it is reasonable to expect the Act to provide certain limitations of access to information from the public domain, the misuse of the limitations stipulated by the Act is contrary to the provision of Article 35 of the Constitution.

The fact that an Act had to be put in place naturally means that the Constitution could not be comprehensive in its provision. Section 17 of the Act widens the scope of the information to include the management of records which include "documents or other sources of information compiled, recorded or stored in written form or in any other manner and includes electronic records<sup>27</sup>". Finally, Section 25 of the Act provides for how regulations may be established to refine the realization of the Act. To date, it is an option that the Executive has not seized.

<sup>22</sup>Article 3 of the Access to Information Act No.31 of 2016.

<sup>23</sup>Section 5 of the Access to Information Act No .31 of 2016.

<sup>24</sup>Section 9 (6) of the Access to Information Act No. 31 of 2016.

<sup>25</sup>Part IV of the Access of Information Act No. 31 of 2016.

<sup>26</sup>Section 6 (1) of the Access to Information Act No .31 of 2016.

<sup>27</sup>Section 17 of the Access to Information Act No .31 of 2016.

### 3.3 The Statute Law (Miscellaneous Amendments) Act No. 18 of 2018

Through the Statute Law (Miscellaneous Amendments) Act No. 18 of 2018, the Government of Kenya amended several provisions of a number of existing statutes, among them the Registration of Persons Act (Cap 107 of the Laws of Kenya). The amendments to the Act established the National Integrated Identity Management System (NIIMS) whose registration process assigns applicants Huduma Namba<sup>28</sup>. Section 9A of the Registration of Persons Act on the establishment of and purposes of NIIMS outlines the following eleven functions: One, “to create, manage, maintain and operate a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya”, two, “to assign a unique national identification number to every person registered in the register”, three, “to harmonize, incorporate and collate into the register, information from other databases in Government agencies relating to registration of persons”, four, “to support the printing and distribution for collection all national identification cards, refugee cards, foreigner certificates, birth and death certificates, driving licenses, work permits, passport and foreign travel documentation, student identification cards issued under the Births and Death Registration Act, Basic Education Act, Registration of Persons Act, Refugees Act, Traffic Act and the Kenya Citizenship and Immigration Act and all other forms of government issued identification documentation as may be specified by gazette notice by the Cabinet Secretary”, five, “to prescribe, in consultation with the various relevant issuing authorities, a format of identification document to capture the various forms of information contained in the identification documents for purposes of issuance of a single document where applicable”, six “to verify and authenticate information relating to the registration and identification of persons”, seven “to collate information obtained under th[e] Act and reproduce it as may be required, from time to time”, eight “to ensure the preservation, protection and security of any information or data collected, obtained, maintained or stored in the register”, nine “to correct errors in registration details, if so required by a person or on its own initiative”, ten “to ensure that the information is accurate, complete, up to date and not misleading” and eleven, “to perform such other duties which are necessary or expedient for the discharge of functions under th[e]Act<sup>29</sup>”.

Significantly, Section 3 of the Registration of Persons Act was amended to include the definition of "biometric" as unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid (DNA) in digital form. Section 5 (1)(g) of the Act was also amended to include Global Positioning Systems (GPS) coordinates as part of the information to be provided on place of residence, and a new paragraph 5 (1)(ha) inserted that provides for biometric data to be kept in the register of all persons in Kenya by the Principal Registrar. While the amendments and the resultant process of digitization of data apply to everyone, including children, Section 2 of the Act does not include children. Thus, by providing that it applies to persons over the age of 18 years; it specifically excludes the application of its provisions to children. Furthermore, with respect to the collection of children’s data, Section 9A (2) of the Act gives NIIMS very generic, wide and ambiguous functions since there are no restrictions regarding the kind of use for the personal data to be collected, including children’s personal data. As such, given children’s vulnerable status, clear distinctions should have been prescribed, distinct from those made regarding data collected from adults, with respect to the collection, use, processing and storage of children’s data.

### 3.4 The Computer Misuse and Cybercrimes Act No. 5 of 2018

The Act was enacted to provide for offences relating to computer systems, to enable timely and effective detection, prohibition, prevention, responsive investigation and prohibition of computer and cybercrimes and

<sup>28</sup>Translated as unique number for service delivery.

<sup>29</sup> The Statute Law (Miscellaneous Amendments) Act No. 18 of 2018.

<sup>30</sup> Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR



to facilitate international co-operation in dealing with computer and cybercrime matters. The law addresses offences such as cyber espionage, computer forgery, computer fraud, false publication, child pornography, cybersquatting, phishing, identify theft, cyber terrorism among others.

Shortly after the President assented to the Act, the High Court issued a conservatory order setting aside the enforcement of 26 sections of the Act, following a petition filed by the Bloggers Association of Kenya (BAKE) and Article 19 challenging the law for violating constitutional provision on freedom of opinion, freedom of expression, freedom of the media, freedom and security of the person, right to privacy, right to property and the right to a fair hearing. The conservatory order was hailed as a win for digital rights enthusiasts in Kenya and also marked a key milestone in the litigation towards respect and realization of digital rights access in the country.

After protracted court battle, the High Court lifted the conservatory order, affirming the 26 sections as constitutional, even though there are still some weaknesses<sup>30</sup>. One, instead of placing more emphasis on crimes found in the cyberspace and those crimes related to ICT systems, transactions and communications, the Act goes above and beyond to deal with free speech. Two, there is no scientific formula of determining what is false or 'fake news'. For example, it will be difficult to determine the authenticity of what is 'fake news' as set out in Sections 22 and 23 of the Act which prohibits publishing false, misleading or fictitious data or information that is intended to cause others to act on them as authentic. Three, the concept of 'fake news' is vaguely defined opening door for varied interpretation, and law enforcers can take advantage of this gap to arbitrary interpret what entails 'fake news'. Further the law enforcers may conceal government misconduct, constrain the expression of critical opinions, and limit free speech of the political opposition, bloggers, human rights defenders and journalists.

### 3.5 The Data Protection Act No. 24 of 2019

Pursuant to the constitutional requirement of Article 31(c) and (d), the right to privacy is given detailed effect by The Data Protection Act No.24 of 2019. The Act establishes the Office of the Data Protection Commissioner appointed by the Public Service Commission responsible for regulation of the processing of personal data and providing for the rights of data subjects and obligations of data controllers and processors. Data Controllers are defined as the persons or entities that determine the purpose and means of processing of personal data, while data processors are the persons or entities that process data on behalf of the Data Controller. The Act also provides for the rights of data subjects including rights of access to personal data and correction or deletion of misleading data. It also details the procedures for rectification and erasure of personal data. Lastly, the Act has an enforcement section which among other provisions provides for a procedure for complaints and offences for unlawful disclosure of data. The Data Commissioner is required to give an Annual Report to the relevant Cabinet Secretary, and may carry out audits of data controllers. The underlying objectives of the Act include inter alia to: regulate the processing of personal data; protect the privacy of individuals; establish the legal and institutional mechanism to protect personal data; and provide data subjects with rights and remedies to protect their personal data from processing<sup>31</sup>.

Section 25 of the Act provides for and summarizes the principles of personal data protection as follows: That personal data is- one, "processed in accordance with the right to privacy of the data subject", two, "processed lawfully, fairly and in a transparent manner in relation to any data subject", three, "collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes", four, "adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed", five, "collected only where a valid explanation is provided whenever information relating to family or private affairs is required", six, "accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay", seven, "kept in a

<sup>31</sup>Section 3 of The Data Protection Act No. 24 of 2019.

form which identifies the data subjects for no longer than is necessary for the purposes which it was collected” and eight “ not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject<sup>32</sup>.” Undoubtedly these principles are consistent with internationally recognized principles and standards espoused in the documents such as the European Union (EU) Guidelines on Data Protection Rights (GDPR), the United Nations Principles on Personal Data Protection and Privacy and principles developed by the Organization for Economic Co-operation and Development (OECD). Further at Section 2, the Act has adopted a definition of personal data which is consistent with the EU GDPR and in the African Union Convention on Cyber Security and Personal Data Protection, namely, any information which is related to an identified or identifiable natural person.

Section 26 of the Act specifically provides for the rights of the data subject, including the right to object to the processing of his or her personal data<sup>33</sup>, while Section 30 (1) of Act provides that the data subject must consent to processing of his or her personal data<sup>34</sup>. These two provisions in the Act further reinforce the protection of personal data.

With respect to the children’s right, the Act provides for the processing of personal data relating to a child under section 33 as follows: One, “Every data controller or data processor shall not process personal data relating to a child unless- consent is given by the child, parent or guardian; and the processing is in such a manner that protects and advances the rights and best interests of the child”. Two, a data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.” Three, mechanisms contemplated under sub-section (2), on age verification and consent, shall be determined on the basis of available technology; volume of personal data processed; proportion of such personal data likely to be that of a child; possibility of harm to a child arising out of processing of personal data; and such other factors as may be specified by the Data Commissioner. Four, “a data controller or data processor that exclusively provides counseling or child protection services to a child may not be required to obtain parental consent as set out under sub-section<sup>35</sup>.” However, the Act has not specified the rights of the child in relation to the personal data collected during minority and upon attaining majority are also not specified, particularly in light of their evolving capacities.

Further, the right to privacy can be limited. In Coalition for Reform and Democracy (CORD) & 2 others V Republic of Kenya & 10 others, the court held that the right to privacy can never be absolute, and that a balancing test has to be applied to determine whether the intrusion into an individual’s privacy is proportionate to the public interest to be served by the intrusion<sup>36</sup>. Finally, the definition of data as “recorded information which is held by a public entity”, is too general and subject to multiple interpretations<sup>37</sup>.

### 3.6 The Proposed Huduma Bill, 2019

The Bill establishes “the National Integrated Identify Management System (NIIMS), to promote efficient delivery of services, to consolidate and harmonize the law on registration of person; to facilitate assigning of Huduma Namba and issuance of identify documents; to facilitate registration of births and deaths<sup>38</sup>.” Specifically, the underlying objective of the Bill include, inter alia: remove duplication from the processes and laws relating to registration of persons; establish a digital national population database to be a single source of foundational and functional data for all resident individuals; provide mechanisms for registration of births, deaths and issuance of identity documents; facilitate transparent and efficient delivery of public services; provide for access and use of the information contained under the NIIMS database; and maintain integrity,

<sup>32</sup>Section 25 of The Data Protection Act No. 24 of 2019.

<sup>33</sup>Section 26 of The Data Protection Act No. 24 of 2019.

<sup>34</sup>Section 30 (1) of The Data Protection Act No. 24 of 2019.

<sup>35</sup>Section 33 of The Data Protection Act No. 24 of 2019.

<sup>36</sup>Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR.

<sup>37</sup>Interview, Digital Protection Advocate, 16 May 2020.

<sup>38</sup>The Huduma Bill, 2019.

confidentiality and security of registration data collected<sup>39</sup>. Unlike Section 9A of the Registration of Persons Act (Revised Version) of 2018 that establishes NIIMS, the Huduma Bill elaborates the various facets of NIIMS such as the components, the database, general design and associated Huduma Namba and Card.

The Bill is a major shift in the process of registration of persons as it, first, subscribes to internationally accepted standards, and secondly, it centralizes all registration systems. The fact that the Bill mandates the Cabinet Secretary to develop steps to mitigate any legal, procedural and social barriers that may limit enrolment is a major achievement to marginalized groups, though the Bill does not adequately address the challenges faced by the same during the registration of person.

The Bill does not provide the reasons behind certain drastic measures, for instance, the enrolment of minors through biometrics from the age of six years<sup>40</sup>. This provision is not consistent with the children's best interests that limit their engagement. Indeed, the existing law requires that children gain access to service through their parents or guardian.

Although the Bill could be praised for its centralist approach in civil registration with a new national ID (the Huduma Namba), there is no policy framework guiding the approach. Further, what is left out are the benefits that will accompany the civil registries in the new system of registration. The Bill imposes duties on citizens with regard to compliance. For instance, Section 16 provides that every person who is enrolled has a duty to notify the NIIMS registration officer to update the particulars of that individual whenever there are any changes in any particular<sup>41</sup>. The Bill imposes harsh sanctions for failure to register or for procuring service without Huduma Namba<sup>42</sup>. It criminalizes any transaction with the government if conducted without the Huduma Namba. The Second Schedule States that any person who commits an enrolment offence is liable to face a period of imprisonment not exceeding five years or a monetary fine not exceeding five million<sup>43</sup>.

The Bill is more technology-inclined. It lacks adequate provisions for public education and awareness on how the technology that will be the primary anchor for the registration process operates. It also lacks provisions for enhancing of informed consent in light of the digital demands of the system. The emphasis placed on the use of fingerprints to enroll or identify an enrolled person is very limiting. Given that it proposes that biometric information cannot be altered by an individual, it could be a tall order for enrolled entries in case the data is stolen or lost from NIIMs. The emphasis on finger may also severely limits persons who due to their work environment have their fingerprints worn out.

The Bill also gives the Principal Secretary (PS) for Interior and Coordination of National Government a lot of powers. Section 45 grants the PS the power to appoint data protection officer<sup>44</sup>. Section 37 mandates the PS the power to facilitate technologically efficient means to ensure proactive access to personal data<sup>45</sup>. Section 25 allows the PS to cancel enrolment of any individual into the NIIMS database<sup>46</sup>. Section 28 allows the PS to designate and facilitate other persons to serve as agents for notification of death or presumed death<sup>47</sup>. Given that the PS is a political appointee, these powers may be misused to serve certain political interests. Finally, the Bill does not provide adequate provisions on how to deal with the protection of the master standard- the biometric information collected in the database.

<sup>39</sup>Section 3 of The Huduma Bill, 2019.

<sup>40</sup>Section 9(a) of Huduma Bill, 2019.

<sup>41</sup>Section 16 of Ibid. Section 16.

<sup>42</sup>Ibid. Part V.

<sup>43</sup>Ibid. Second Schedule.

<sup>44</sup>Ibid. Section 45

<sup>45</sup>Ibid, Section 37

<sup>46</sup>Ibid, Section 25

<sup>47</sup>Ibid, Section 28

# CHAPTER FOUR

## ANALYSIS OF RECENT HUDUMA JUDGEMENT

*The Huduma petition was an amalgamation of petitions filed by the Nubian Rights Forum, the Kenya Human Rights Commission and the Kenyan National Commission on Human Rights aggrieved by the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 which sought to establish a National Integrated Identity Management System (NIIMS). The petitioners claimed that it was passed in violation of the Constitution and in bad faith and posed serious and immediate threats to fundamental rights and freedoms protected under the Bill of Rights.<sup>48</sup> This analysis of the judgement thus draws from the following grounds of the petition: that the registration process infringed on the rights to privacy; that Kenya lacks a comprehensive data protection law; that the registration process lacked legal basis; and that the process would further marginalize persons who have not acquired the primary documents required to register for Huduma Namba.*

### 4.1 The Registration Process Infringed on the Rights to Privacy

Two questions were raised in the judgement: Whether the personal information collected is excessive, intrusive, and disproportionate, and whether the registration process violated children's right to privacy.

#### **Whether the personal information collected is excessive, intrusive, and disproportionate**

Two facets of arguments were raised with respect to this question. The first facet was that the provisions for collection of biometric data by the amendments was intrusive and unnecessary. Linked to the first facet

<sup>48</sup>The petitioners were supported by Muslims for Human Rights, Haki Centre, Law Society of Kenya and Inform Action which were joined to the proceedings as the 3rd, 4th, 5th and 6th Interested Parties respectively; the respondents in the Consolidated Petitions were the Honourable Attorney General (the 1st Respondent); the Cabinet Secretary, Ministry of Interior and Co-ordination of National Government (the 2nd Respondent); the Principal Secretary, Ministry of Interior and Co-ordination of National Government (the 3rd Respondent); the Director of National Registration (the 4th Respondent); the Cabinet Secretary for Information, Communication and Technology (the 5th Respondent); the Speaker of the National Assembly (the 6th Respondent); and the Kenya Law Reform Commission (the 7th Respondent), and other interested parties were The Child Welfare Society of Kenya, Ajibika Society, Bunge La Mwananchi, International Policy Group and Terror Victims Support Initiative being the 1st, 2nd, 7th, 8th and 9th.



of the question is the second facet that the data collected pursuant to the amendments is not supported by the stated purposes of NIIMS<sup>49</sup>. The court interrogated the subject matter and scope of the right to privacy including information, and concluded that biometric data and Global Positioning System (GPS) coordinates required by the amendments were personal, sensitive and intrusive data that required protection. In the court's wisdom, it found that the amendments impose obligations on the state agencies to institute personal data safeguards<sup>50</sup>.

Further, the court held that the biometric data collected was not contradictory to the purposes of NIIMS as contained in Section 9A of the Registration of Persons Act, and that the two functionalities of NIIMS as identification and verification system justified the establishment of NIIMS and the other existing identification and registration databases. Therefore, from an identification and verification perspective, NIIMS was important because the biometric data collected was key in identification, and will serve verification purposes in relation to other existing databases<sup>51</sup>. Finally, the court concluded that the stated benefits of NIIMS were in the public interest and not unconstitutional<sup>52</sup>.

### Whether there is a Violation of Children's Right to Privacy

The court observed that it was clear that Section 9A of the Registration of Persons Act on the purposes of NIIMS was inconsistent with Section 2 of the Registration of Persons Act, 2012 and the two cannot exist with respect to the application of NIIMS to children. Upon considering the rules of statutory interpretation on implied amendment, the court found that Section 2 was amended by Section 9A, with regard to its application to NIIMS, thereby solving the above inconsistency. Therefore the court concluded that Section 9A of the Registration of Persons Act and NIIMS applies to children<sup>53</sup>. Also applicable to children were the general principles and protections that apply with regard to the right to informational privacy and the biometric data collected under NIIMS, because children's rationality is limited because of their limited exposure and education<sup>54</sup>. Despite NIIMS being applicable to children, there were no special provisions in the amendments, and no regulations that govern how the data relating to children was to be collected, processed and stored in NIIMS. The court concluded therefore that the legislative framework on the protection of children's biometric data collected in NIIMS as inadequate.

## 4.2 Kenya Lacks a Comprehensive Data Protection Law

The court considered whether there were adequate legal safeguards and data protection frameworks, noting that the protection of personal data is a function of a legal, regulatory and institutional framework. This consideration is important in the case of NIIMS where the state agencies would be exposed to huge personal data, and that data subjects would be constrained from determining how the information about their live would be utilized<sup>55</sup>.

Whereas the court found that the Data Protection Act No 24 of 2019 was consistent with internationally accepted standards, it was observed that still there were several provisions in the Act that needs operationalization through regulations. For instance, under what circumstances would the Data Commissioner exempt the operation of the Act, and may grant data sharing codes on the exchange of personal data between government departments. These regulations have implications on the protection and security of personal data.

It was observed that once in operation, Data Protection Act requires effective implementation and enforcement. For effective implementation of the Act, an implementation framework is key. For instance, the appointment of independent Data Commissioner by Public Service Commission, registration of the data

<sup>49</sup>Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR, p.220.

<sup>50</sup>Ibid.

<sup>51</sup>Ibid.

<sup>52</sup>Ibid.

<sup>53</sup>Ibid, p.221.

<sup>54</sup>Ibid.

<sup>55</sup>Ibid.

controllers and enactment of operational regulations. The court found that although there existed a legal framework on the collection and processing of personal data, data safeguards requires the operationalization of the legal framework<sup>56</sup>.

Pertaining the safety and security concerns of the design of NIIMS, the court concluded that all biometric systems, whether centralized or decentralized, and whether using closed or open source technology, need tight security policy framework on its protection and security consistent with internationally accepted principles. The court also observed that the biometric data and personal data in NIIMS should only be utilized once there is an appropriate legal framework in which sufficient safeguards are built in to protect fundamental rights<sup>57</sup>.

To the extent that State agencies did not dispute that there was no specific regulatory framework governing the operations and security of NIIMS and that they reported that only a few measures had been put in place to safeguard the data collected by NIIMS and the security of the system, the court concluded that the legal framework on the operations of NIIMS was inadequate, consequently posing risk to the security of data collected in the system<sup>58</sup>.

### 4.3 The Registration Process Lacked Legal Basis

The court considered whether the amendments were unnecessary, unreasonable and unjustifiable limitation. The court observed that given the specificity of the information that DNA may disclose and the harm disclosure may cause both to the data subject and other family members, DNA information needs legislation. Similarly, the court founds utilization of GPS requires specific legislation in light of the privacy risk identified in terms of their potential to be used to track and identify a person's location. As such the court found that the collection of DNA and GPS coordinates in the amendments, without specific legislations was not justifiable.

To the extent that lack of adequate legislative framework for safeguarding personal data is clearly a violation of the right to privacy in light of the associated risks to unauthorized access and other data breaches, the court found that the lack of a comprehensive legislative framework when collecting personal data under the amendments, was contrary to the principles of democratic governance and the rule of law, and thereby unjustifiable<sup>59</sup>.

### 4.4 The Process Would Marginalize Persons who have not acquired the Primary Documents Required to Register for Huduma Namba

Two limbs of arguments were presented with regard to allegation of denial of the right to equality and non-discrimination. The first limb of the argument alleged that the amendments and the implementation of NIIMS will reinforce the current discrimination against members of the Nubian community and other marginalized groups. The second limb of the argument alleged that the amendments making it mandatory for everybody to acquire Huduma Namba, a condition precedent to obtaining government services, was unconstitutional. On the question of discrimination against the Nubian Community, the court found that the amendments did not address the issue of distinction between members of the Nubian community and other marginalized groups relative to non-marginalized Kenyans<sup>60</sup>, thus the court was unable to discern violation of the right to equality and non-discrimination from the evidence adduced<sup>61</sup>.

<sup>56</sup>Ibid, p.222.

<sup>57</sup> Ibid.

<sup>58</sup>Ibid.

<sup>59</sup>Ibid

<sup>60</sup>Ibid, p.223

<sup>61</sup>Ibid.





As to whether obtaining the Huduma Namba was mandatory, failing which one will be denied government services, and thus leading to violation of the right to non-discrimination, the court found that whereas it was unanimously agreed by all the parties that digital data promises to transform Kenya, what is important is to ensure that no one is excluded from the NIIMS and associated services. This could be necessitated by lack of identity documents, or lack of or poor biometric data. The court noted that there could be a section of the population at the risk of exclusion<sup>62</sup>.

Therefore, the court concluded that there was need for a clear regulatory framework that would address the possibility of exclusion in NIIMS. The framework should address how people without access to identity documents or with poor biometrics would be registered in NIIMS. Although the court recognized the possibility of this exclusion, however, it did not find adequate reason to render NIIMS unconstitutional<sup>63</sup>.

---

<sup>62</sup>ibid.

<sup>63</sup>ibid.

# CHAPTER FIVE

---

## PERCEPTIONS, IMPLEMENTATION AND IMPACT OF THE RELEVANT LEGISLATION AND POLICY PROPOSALS

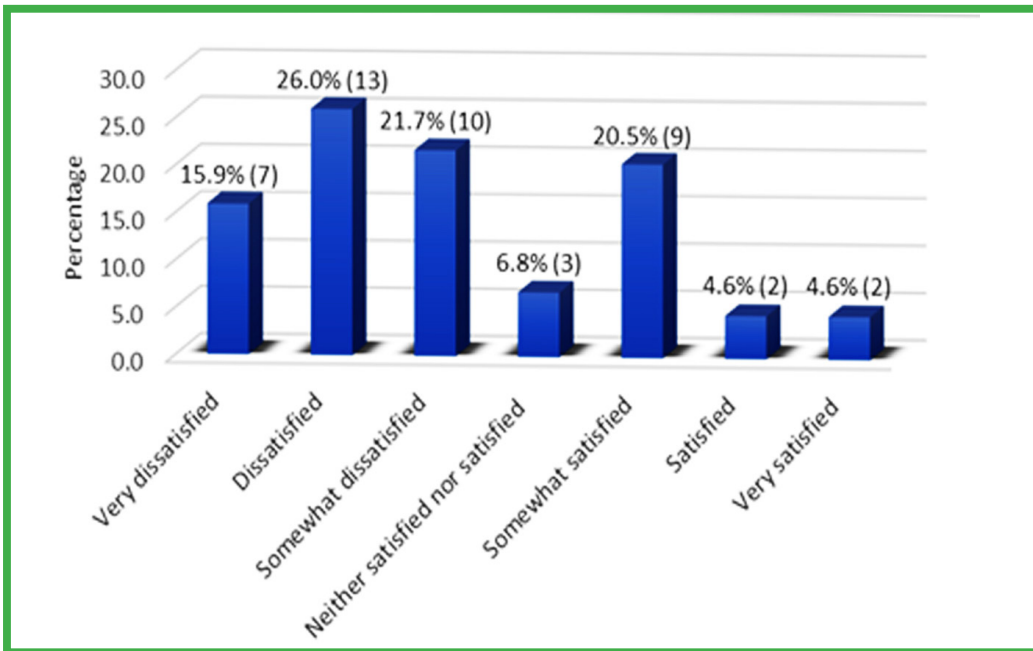
*This chapter presents findings on perceptions about the implementation and impact of the relevant legislation and policy proposals. Perceptions vary over time and may differ substantially among stakeholders. How change is reflected among stakeholders then becomes a causal link between the legal framework and action. This chapter focuses on the perceptions, implementation and impact of Access to Information Act, 2016; Computer Misuse and Cybercrime Act, 2018, Data Protection Act, 2019 and NIIMs and its associated Huduma Namba.*

### 5.1 Right to Access to Information

Under the right to access to information, the study sought to find out whether respondents were satisfied with the implementation of Article 35 of the Constitution. As indicated in figure 1, a majority of respondents (13) reported that they were dissatisfied with the implementation of the constitutional provision, while 7 reported that they were very dissatisfied. Only two respondents reported that they were very satisfied, while another two reported that they were satisfied. High percentage of dissatisfaction may be indicative of general disillusionment with the implementation of Chapter Four on the Bill of Rights.

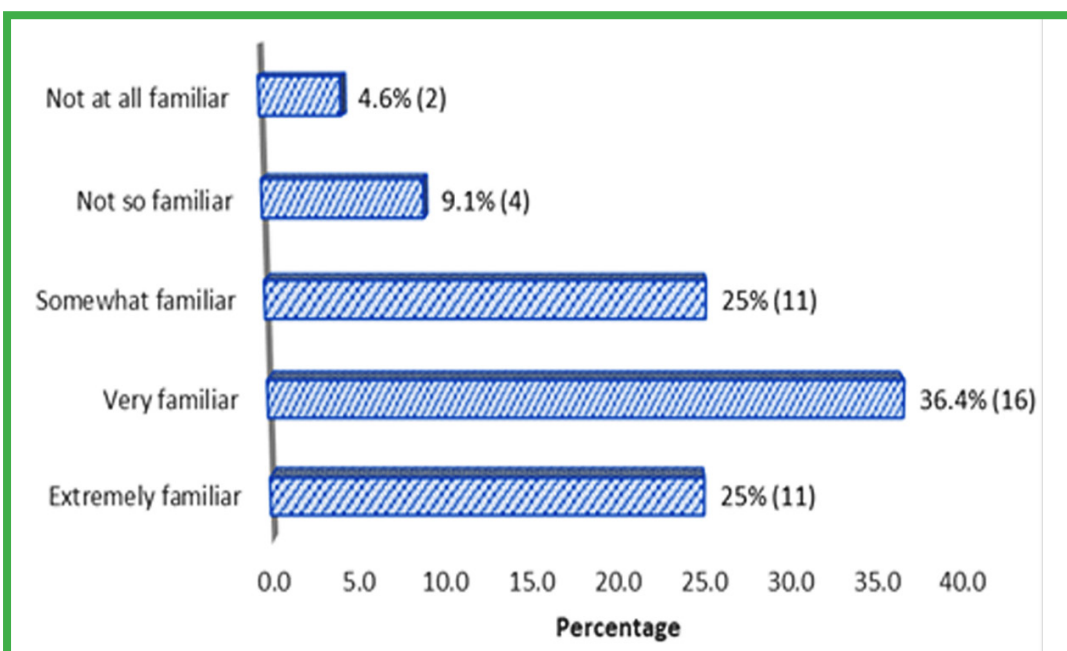


**Figure 1: Satisfaction Level with the Implementation of Article 35**

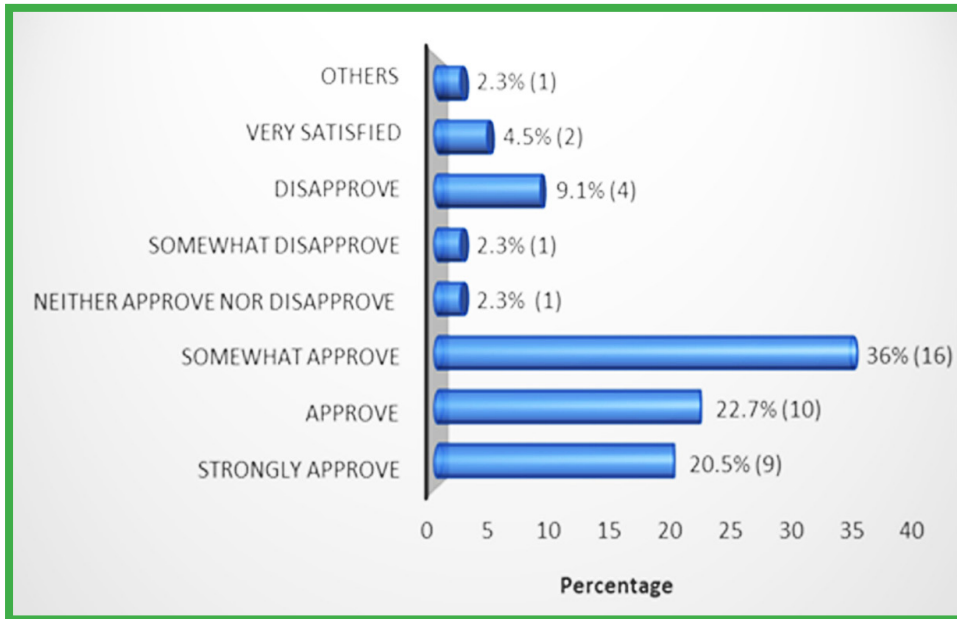


Despite considerable dissatisfaction with the implementation of Article 35, a majority of respondent (16) were very familiar with the existence of Access to Information Act, 2016, while 11 were extremely familiar as shown in figure 2. Awareness of the existence of the law could be due to access to political information and knowledge and participation in civic organizations. The awareness could also be advanced through one’s socio-economic status given that virtually all the respondents were purposively selected from an elite group knowledgeable or have closely worked with information technology platforms. When we turn to the extent of satisfaction with the implementation of the Act, there was mixed result. As indicated in figure 3, 36 % of the respondents reported that they somewhat approved the implementation, implying that although some level of implementation is on course, it is not worth to celebrate as there could be some elements of the law that needs to be reconsidered. Those who approve the implementation of the Act stood at 22.7% while those that strongly approved was 20.5%.

**Figure 2: Familiarity with the existence of Access to Information Act, 2016**

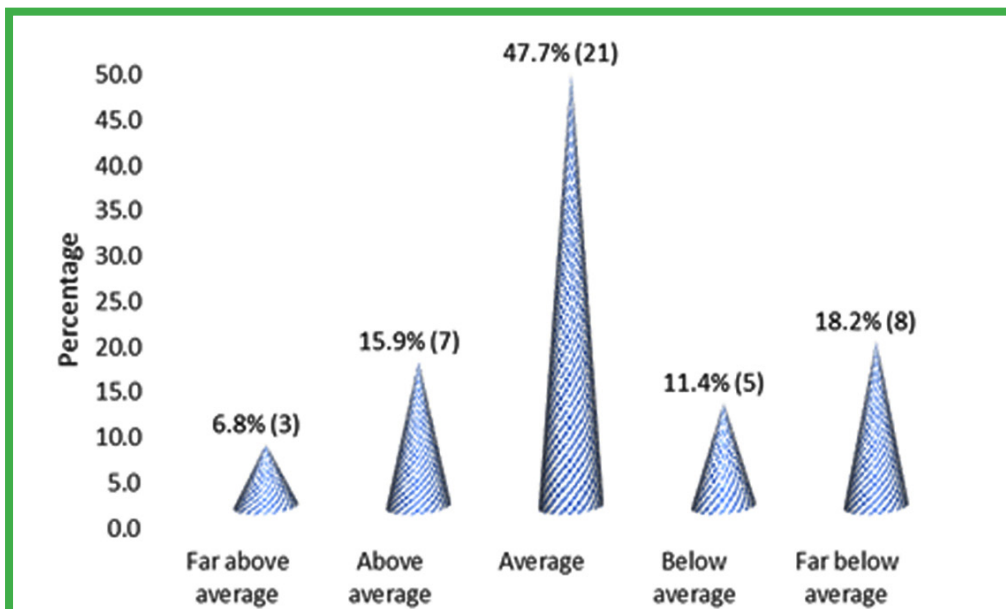


**Figure 3: Extent of satisfaction with the implementation of the right to information access since the enactment of the Act**



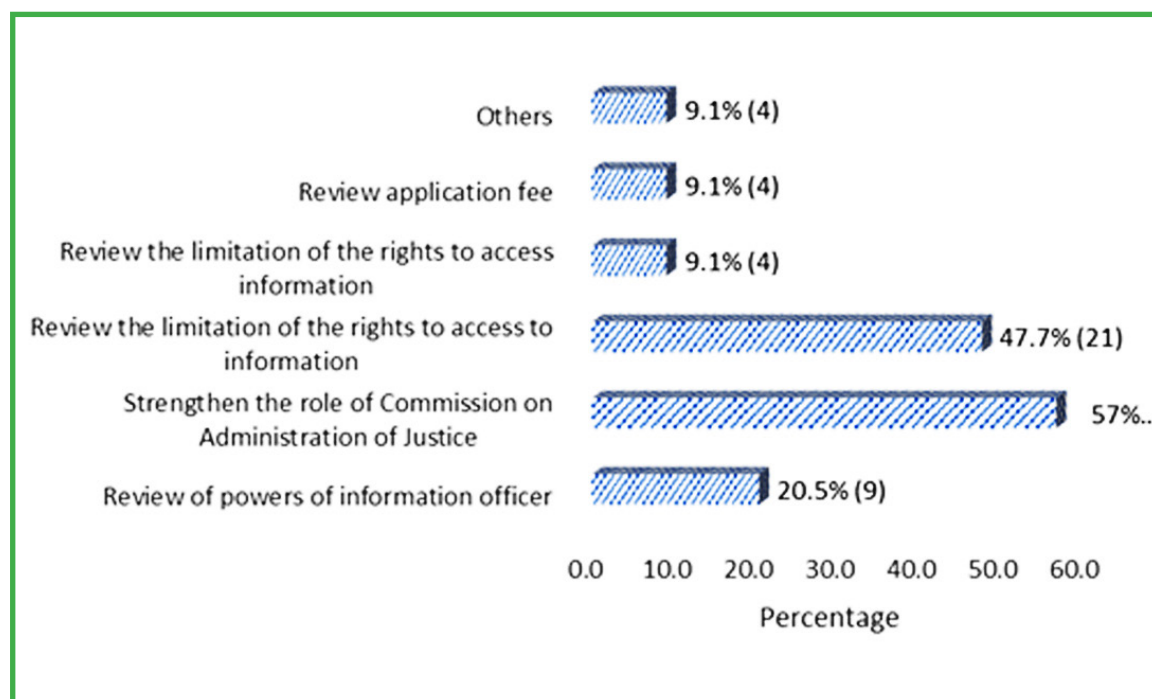
Turning to the impact of the implementation of the Access to Information Act 2016, as shown in figure 4 almost half of the respondents considered that indeed there have been some positive changes. In other words, the enactment of the Act has in some ways assisted citizens to access information that they would not have otherwise accessed. It could also be interpreted that despite the Bill of Rights in the Constitution of Kenya being hailed as one of the progressive frameworks, there wasn't much implementation to safeguard right to access to information as enshrined in the Constitution. As such, 47.7% indicate that the implementation of the Act has further broadened the constitutional foundation of promoting efficient, effective, transparent and accountable governments. Given that only three years have elapsed since its enactment, if gray areas in the Act are reviewed in future, it may considerably safeguard the rights to access to information. However, attempts to validate the extent of some positive change proved challenging as an interviewed government official reported that many of government departments do not keep accurate records of the information sought by outsiders, thereby difficult to assess the impact of implementation of the Act to citizens.

**Figure 4: Impact of the Implementation of Access to Information Act, 2016**



It is for above optimism that the study went ahead to finding the specific kind of reviews that should be made in the Act. As indicated in figure 5, a majority of respondents (56.82%) suggested that the role of Commission on Administration of Justice should be strengthened, implying that the constitutional body empowered to oversight and enforce the rights to access to information has not been up to its task. That was closely followed by suggestions that the limitations of the rights to access information set in the Act should be reviewed (47.73%). Others (20.45%) suggested that the power of information officers should be reviewed; still other respondents (9.09%) suggested that application fees should be reviewed. In addition, 9.09% specified two reviews that should be made in the Act. One, that the Act should allow the aggrieved person to approach the court in instances where his/her request for information is refused. Two, that the Act should incorporate the notion that public interest overrides a refusal and that information officer should be obliged to mandatory disclose relevant information to the public in circumstances where it is provided that the disclosure would reveal evidence of the contravention of the law or serious public safety. Regarding the balance between seeking redress from the court and the general limitations in the Act, a legal expert on the subject informed the researcher that the limitations have been a concern of the position of the court in enforcing the limitations of the rights, while pertaining public interest, he pointed out the challenges that lies in deciding what constitutes public interest<sup>64</sup>. Indeed Raboy and Abramson (1988, p.329) observed that the concept of public interest is essentially contested, despite its popularity among policy-makers.

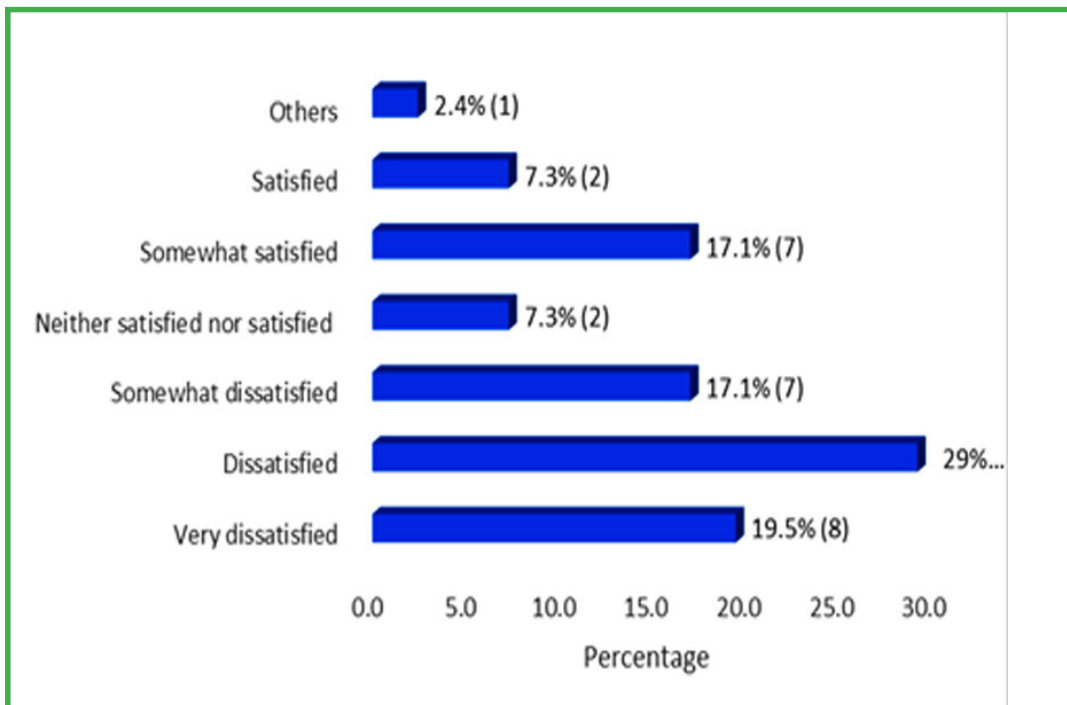
**Figure 5: Suggestions of the review of the Act**



## 5.2 Right to Privacy

Turning to right to privacy, the study sought to find out whether respondents were satisfied with the implementation of Article 31 of the Constitution. Like in the case of the right to access information, as shown in figure 6, a majority of respondents (29%) reported that they were dissatisfied with the implementation of the Article, while 19.5% reported that they were very dissatisfied. Only two respondents reported that they were satisfied, while one respondent reported not being in a position to evaluate the Article. Similarly, high percentage of dissatisfaction may be indicative of general disillusionment with the implementation of Chapter Four on the Bill of Rights.

<sup>64</sup>Personal interview, legal expert, 14 April 2020.

**Figure 6: Satisfaction with the implementation of Article 31 of the Constitution**

Despite considerable dissatisfaction with the implementation of the Article 31, as indicated in figure 7, majority of respondents (34.2%) were very familiar with the existence of Data Protection Act, 2019, 26.8% of respondents were somewhat familiar with the Act and 17.1% of the respondents were extremely familiar.

As for Computer Misuse and Cybercrimes Act, 2018, at least more than 85% of the respondents reported familiarity with the Act as illustrated in figure 8. The higher familiarity of the Computer Misuse and Cybercrimes Act than Data Protection Act can be understood from two factors. One is the time dimension factor, given that the former was enacted earlier than the latter. Two, protracted court battle courtesy of a petition filed by the Bloggers Association of Kenya (BAKE) popularized the Act thereby creating awareness among citizens. Just like in the case of Access to Information Act, familiarity with these two Acts could be attributed to access to political information and knowledge and participation in civic organizations. As indicated earlier, the awareness could also be advanced through one's socio-economic status given that virtually all the respondents were purposively selected from an elite group knowledgeable or have closely worked with information technology platforms. Looking at the extent of satisfaction with the implementation of the two Acts, they appear to somehow follow similar patterns as indicated in figures 9 and 10. Whereas Data Protection Act reported 12.2, 39, and 17.1, Computer Misuse and Cybercrimes Act reported 9.8, 26.8 and 12.2 respectively for very dissatisfied, dissatisfied and somewhat satisfied. It is surprising that the Data Protection Act reported favourable rating of satisfaction than Computer Misuse and Cybercrimes Act yet, the latter was enacted earlier than the former. Overall, dissatisfaction with the implementation implies that several provisions of the laws that are yet to be operationalized, and therefore constraining enjoyment of the constitutional foundations of the rights to privacy.

Figure 7: Familiarity with the existence of Data Protection Act, 2019

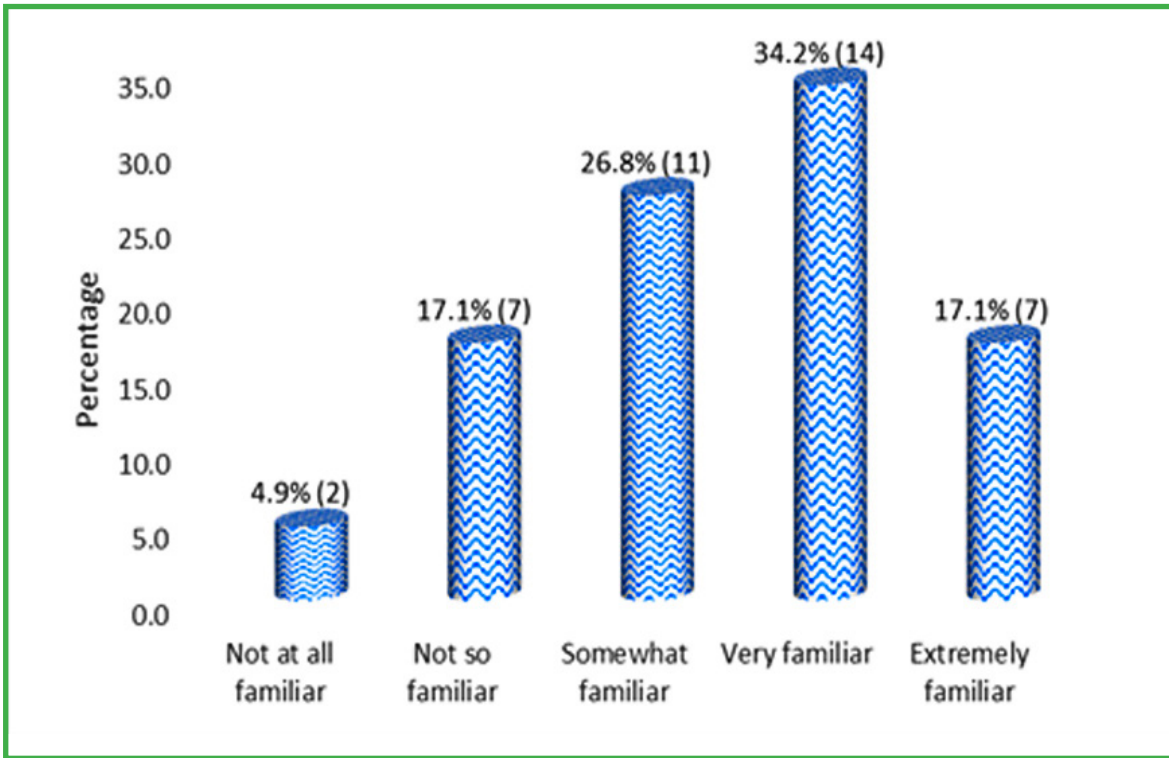


Figure 8: Familiarity with existence of Computer Misuse and Cybercrimes Act, 2018

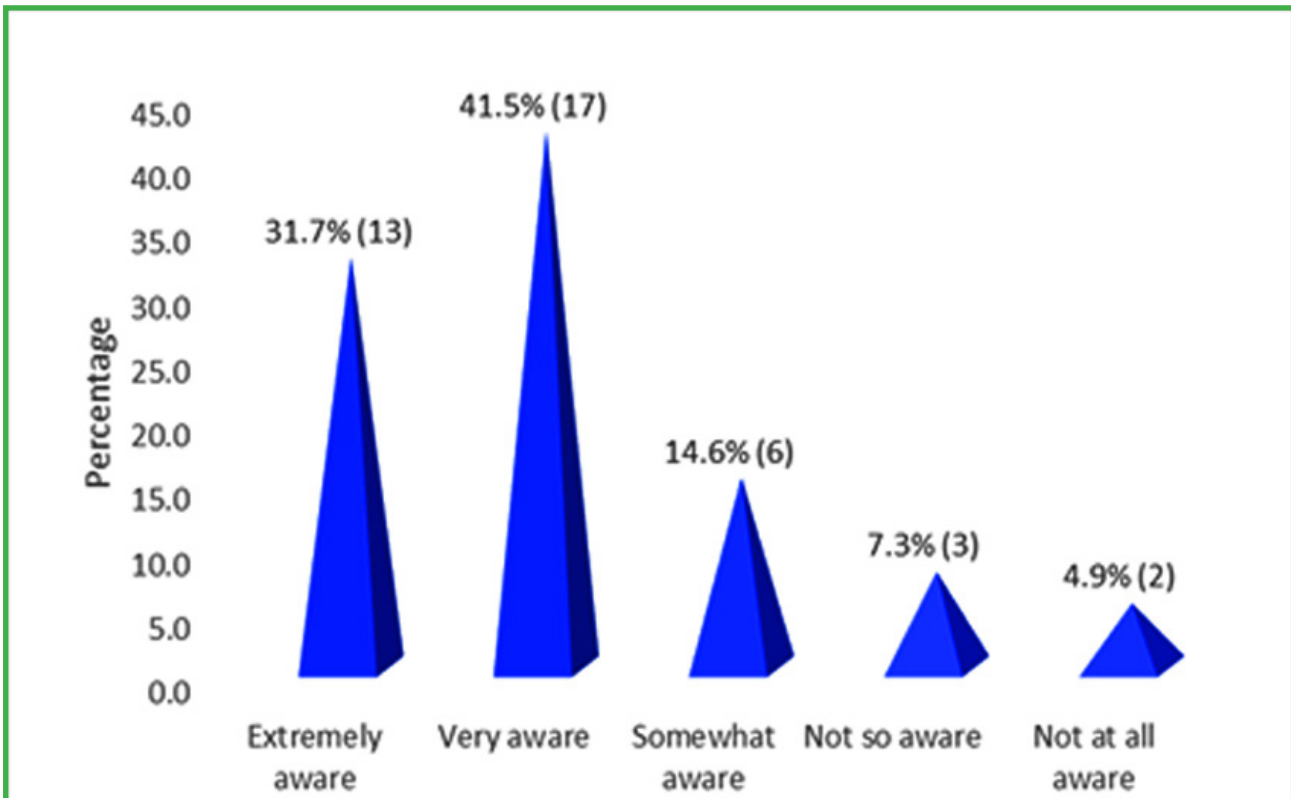


Figure 9: Satisfaction level with regard to the Implementation of the Data Protection Act, 2019

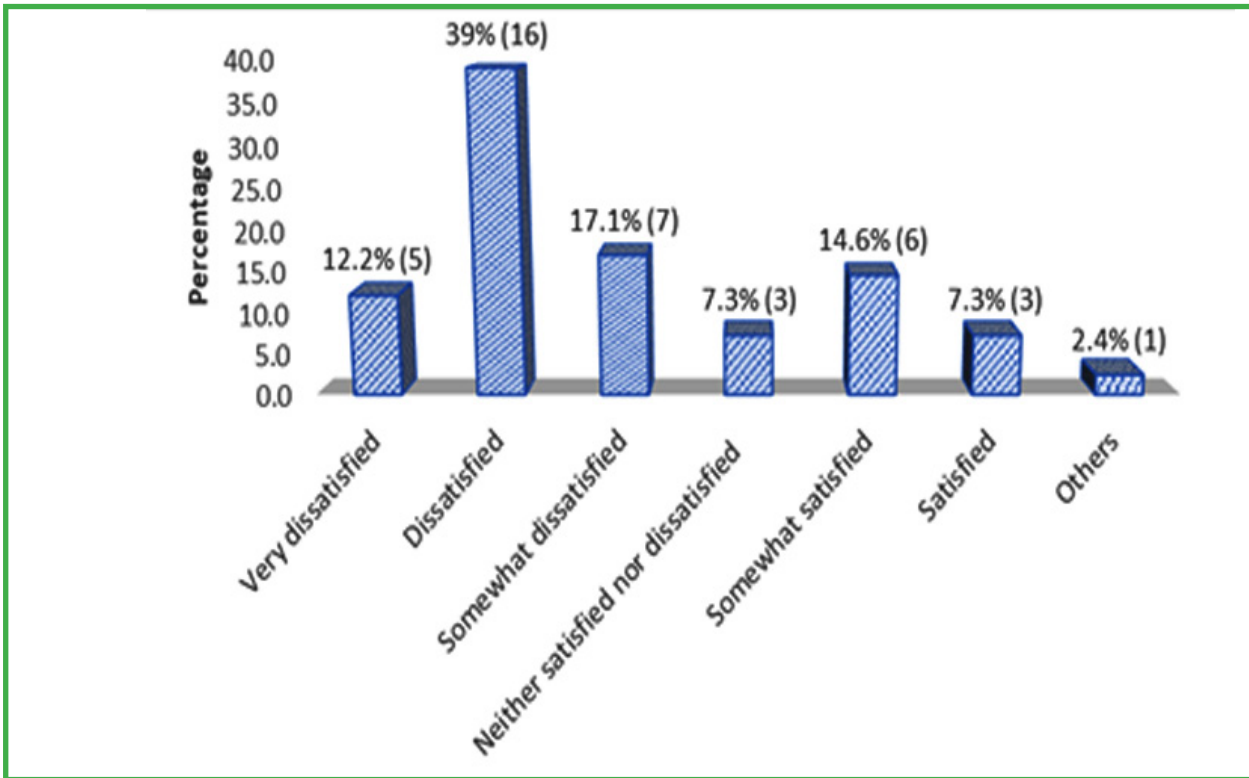
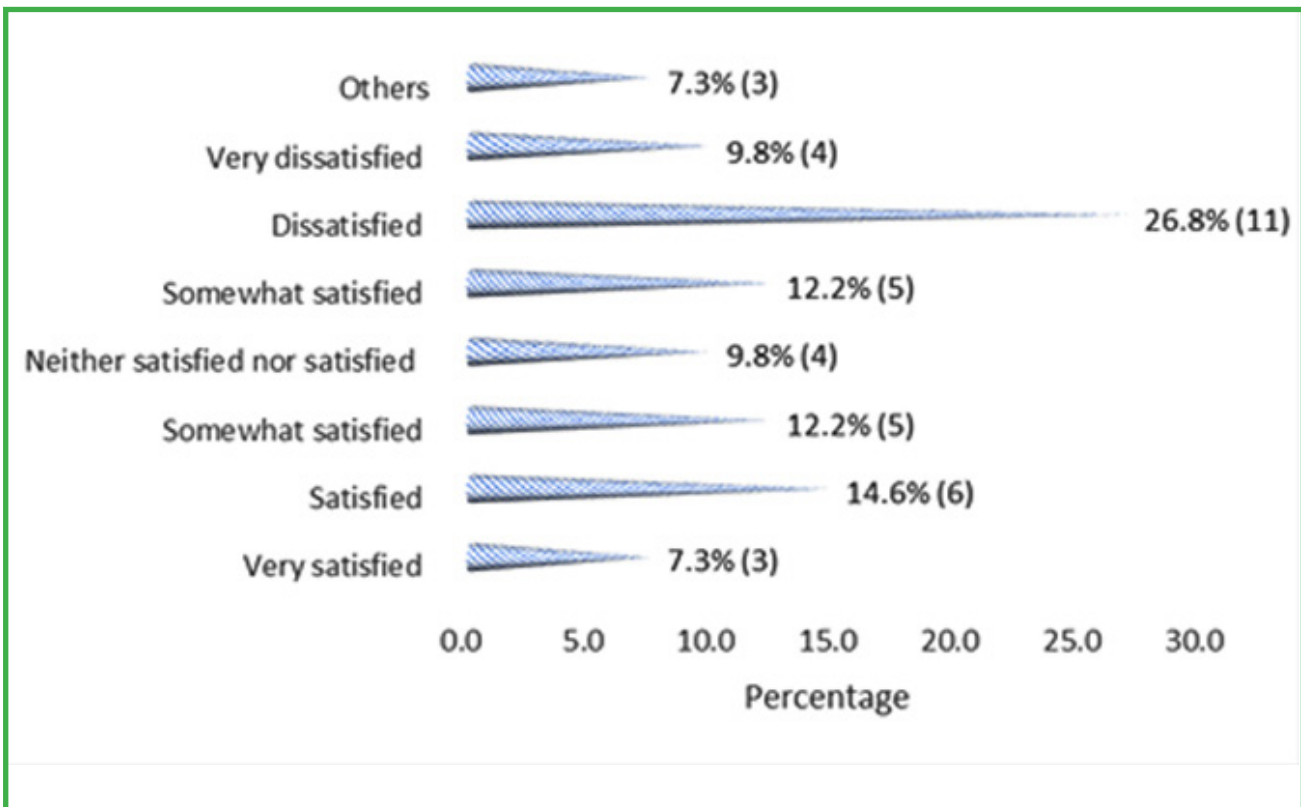


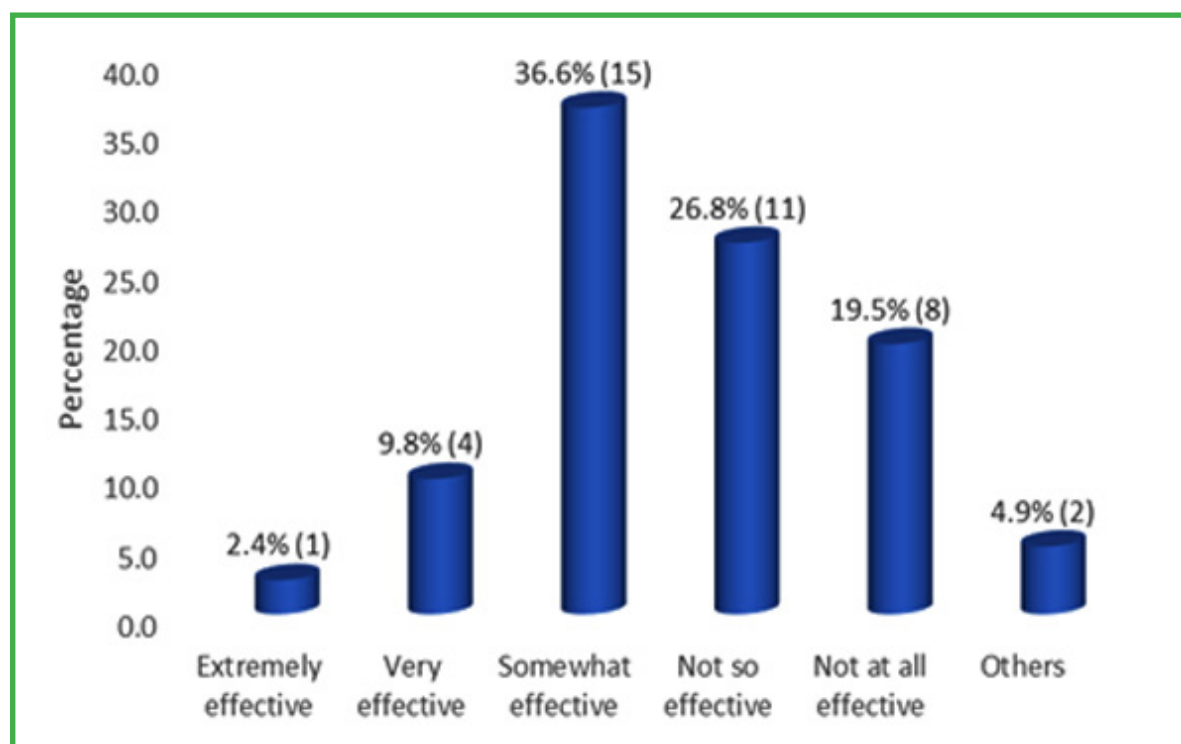
Figure 10: Satisfaction level with the Implementation of Computer Misuse and Cybercrime Act, 2018





The study further sought to find out the impact of the two Acts. Despite dissatisfaction, as shown in figure 11, 36.59%, 9.76% and 2.44% of the respondents respectively reported that the Acts were somewhat effective, very effective and extremely effective. It implies that although the Acts are relatively new, their effects have already been felt and if some gray areas could be looked into, then they promise to safeguard the rights of privacy. For instance, in the case of Data Protection Act, it provides that a data controller or data processor must carry out a data protection impact assessment that is “an assessment of the impact of the envisaged processing operations and the protection of personal data”. Section 31 (3) of the Act provides that the data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject. Section 31(5) of the Act requires that the data impact assessment report should be submitted sixty days prior to the processing of data. At the moment the government of Kenya is yet to appoint a Data Commissioner<sup>65</sup>, what is more, it is not feasible to have data impact assessment reports done sixty days prior to processing of the data.

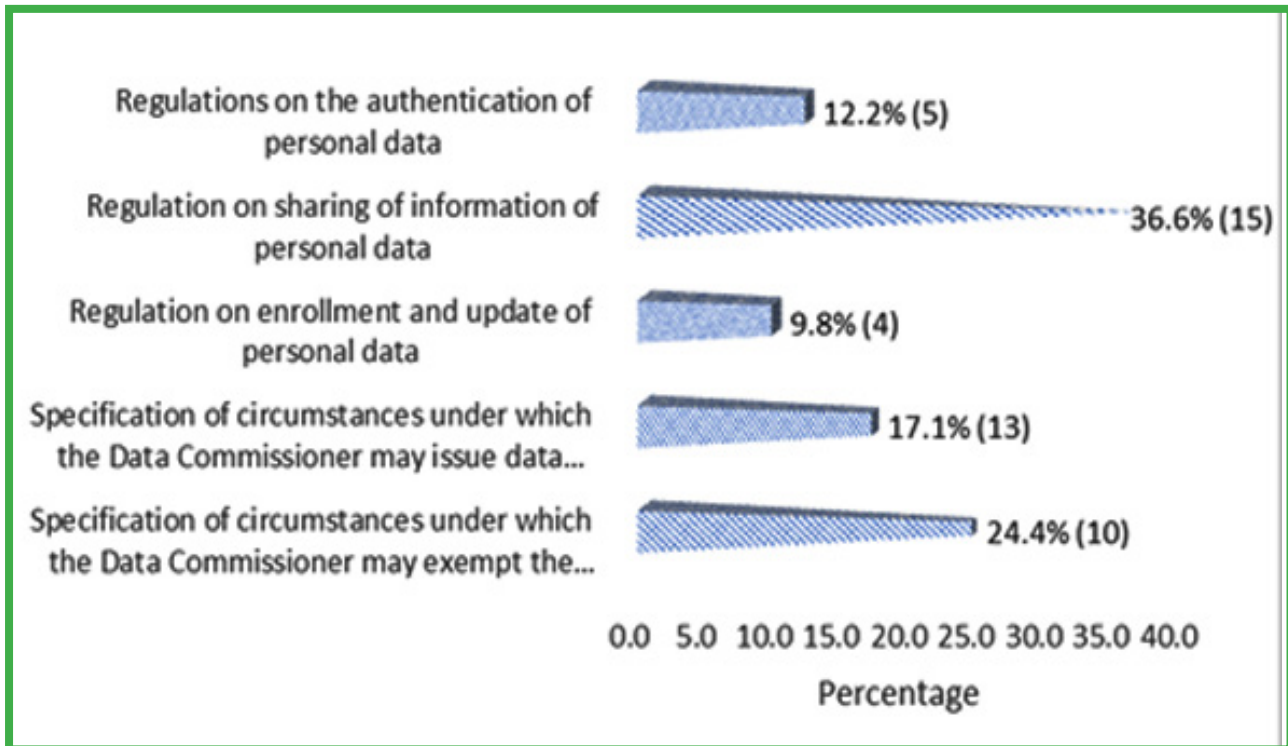
**Figure 11: Impacts of Computer Misuse and Cybercrimes Act, 2018 and the Data Protection Act 2019**



Furthermore, when asked the kinds of regulations that should be made to enhance the right to privacy, as shown in figure 12 36.59% suggested regulation on sharing of information of persons, 24.39% suggested specification of circumstances under which the Data Commissioners may exempt the operation of the Act. Others (12.2%) suggested regulations on the authentication of personal data, 17.07% suggested specification of circumstances under which the Data Commissioners may issues data sharing code on the exchange of personal data between government departments and 9.76% suggested regulations on enrollment and update of personal data. One of the key informants observed that Kenya could learn a lot from India which managed to provide regulatory framework through the Aadhaar Act India by providing sufficient safeguards through regulations on enrolment and update, authentication and sharing of information.

<sup>65</sup>The position was advertised by Public Service Commission.

**Figure 12: Suggestions on regulation to enhance the right to privacy**



### 5.3 NIIMs and associated Huduma Namba and Card

The study also collected views on the NIIMs regarding its accuracy of data, data controls, security of data, extent of lawfully, transparency and fairness in the utilization of data and implementation cost and sustainability. Regarding accuracy, as indicated in figure 13 a majority of the respondents (11) were not sure whether the accuracy of the system would be high or low, five of the respondents believed that the system accuracy would be somewhat high while six of the respondents believed that the system accuracy would be high. With regard to data controls, as shown in figure 14 the dominant view oscillated towards the system not being effective. As for the security of the data, as indicated in figure 15 a majority of respondent did not trust that the system will secure data. Equally, a majority of respondents did not believe that the system would be lawful, transparent and fair and still many believed that the implementation cost of the system would be too high and not sustainable as demonstrated in figure 16 and 17 respectively. Finally, a majority of respondents strongly disapproved of the proposed mandatory uses of Huduma Namba and Card when transacting with government as shown in figure 18



Figure 13: Accuracy of data in the NIIMs

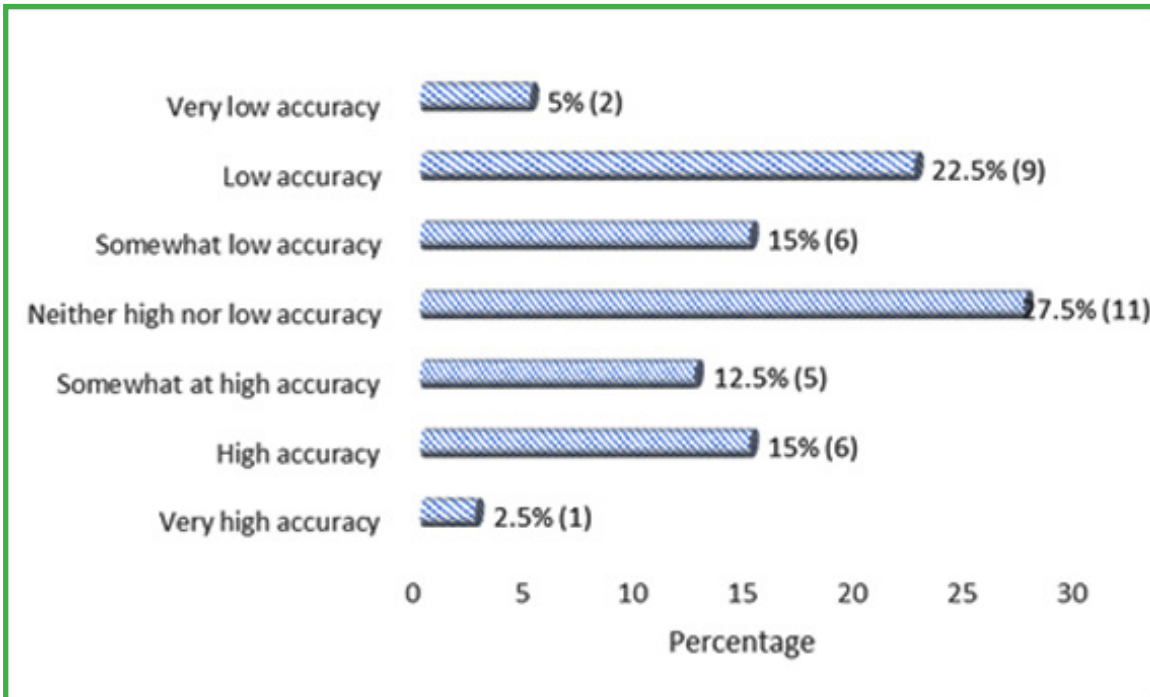


Figure 14: Data controls in the NIIMs

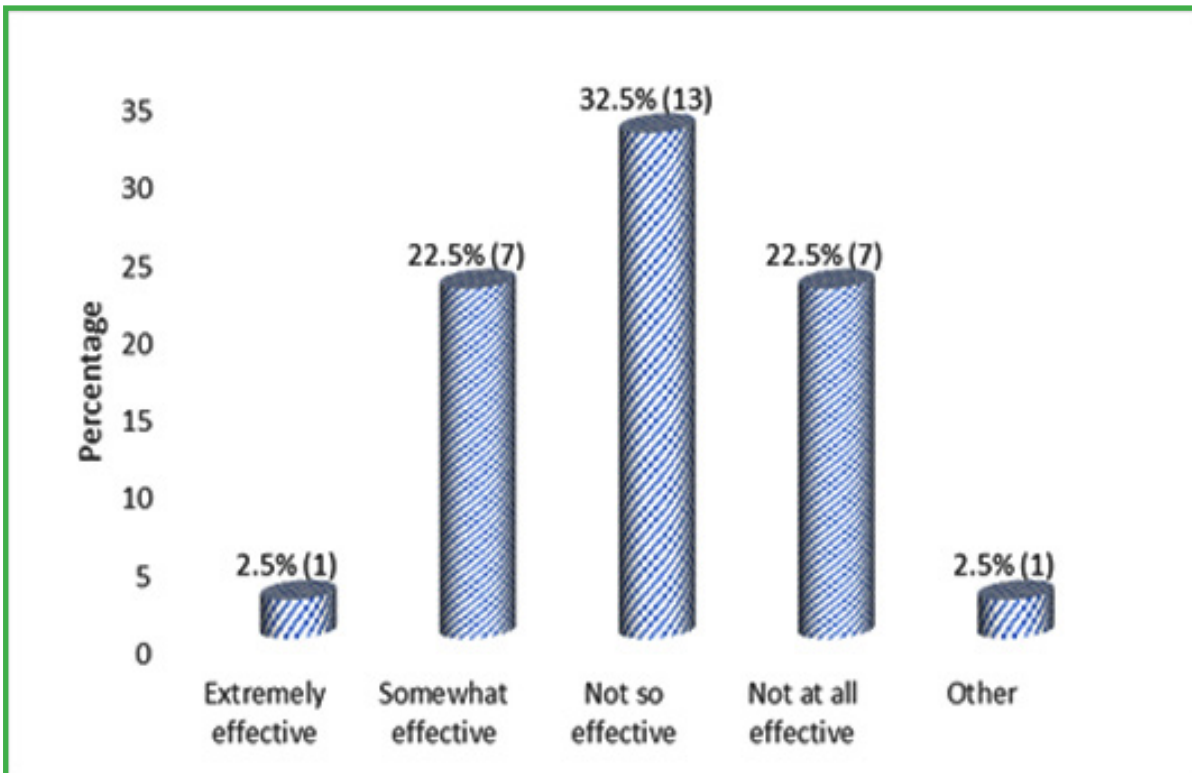


Figure 15: Security of data in the NIIMS

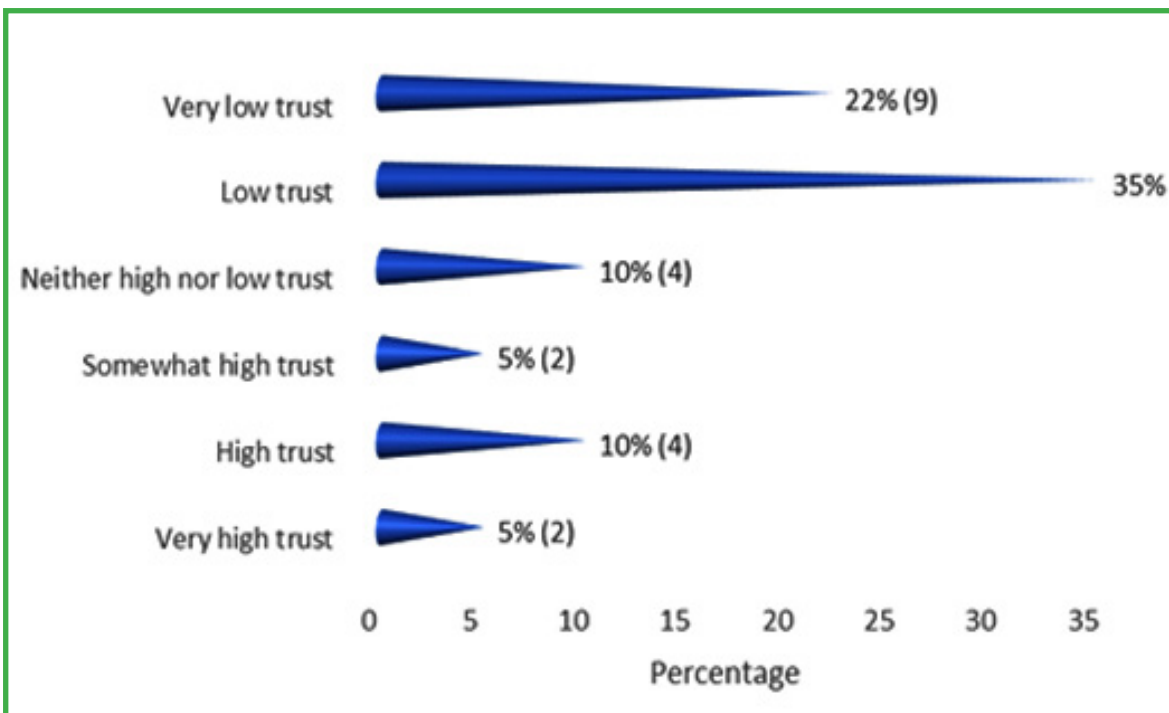


Figure 16: Extent of lawfully, transparency and fairness in the utilization of data in the NIIMS

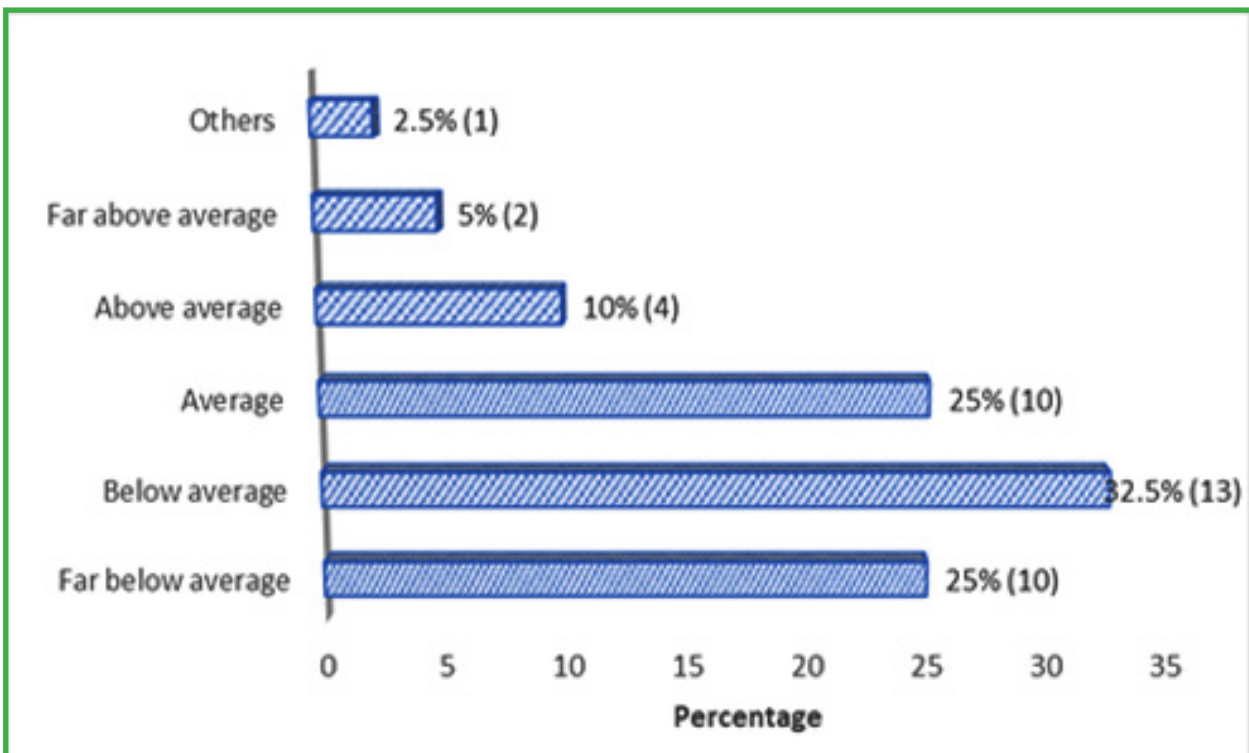


Figure 17: Implementation cost and sustainability of the NIIMs

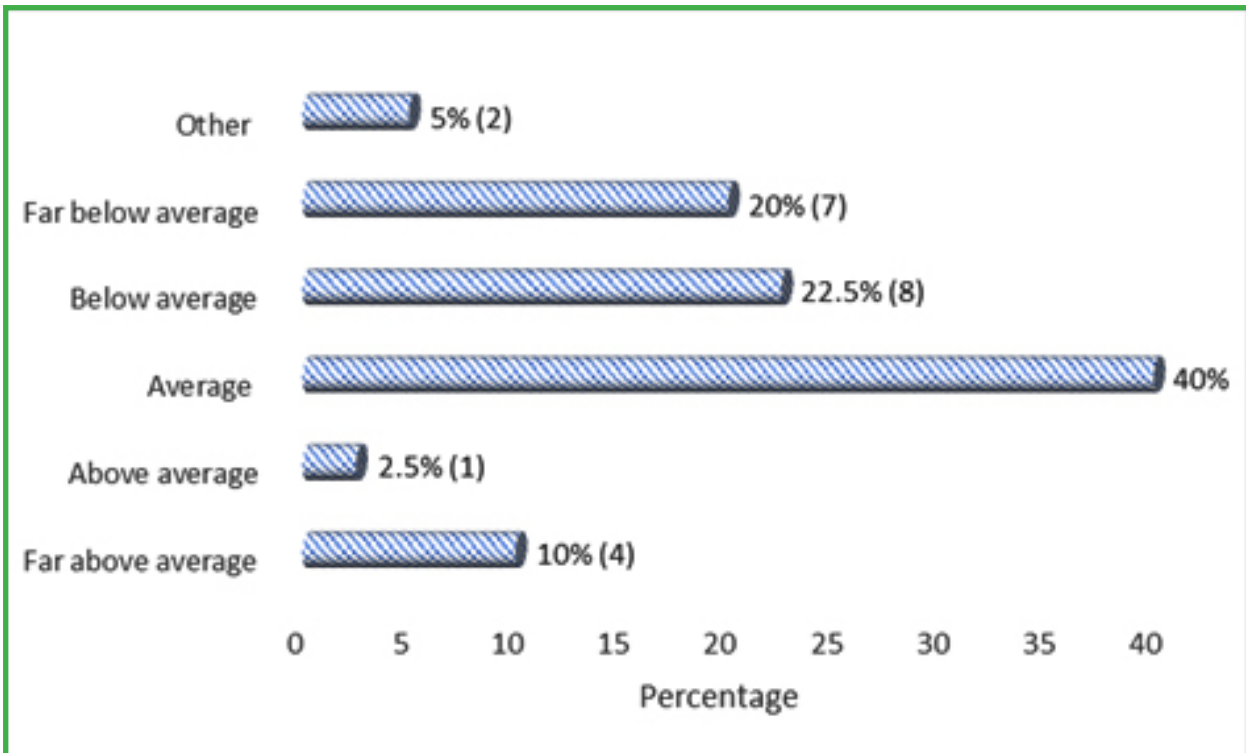
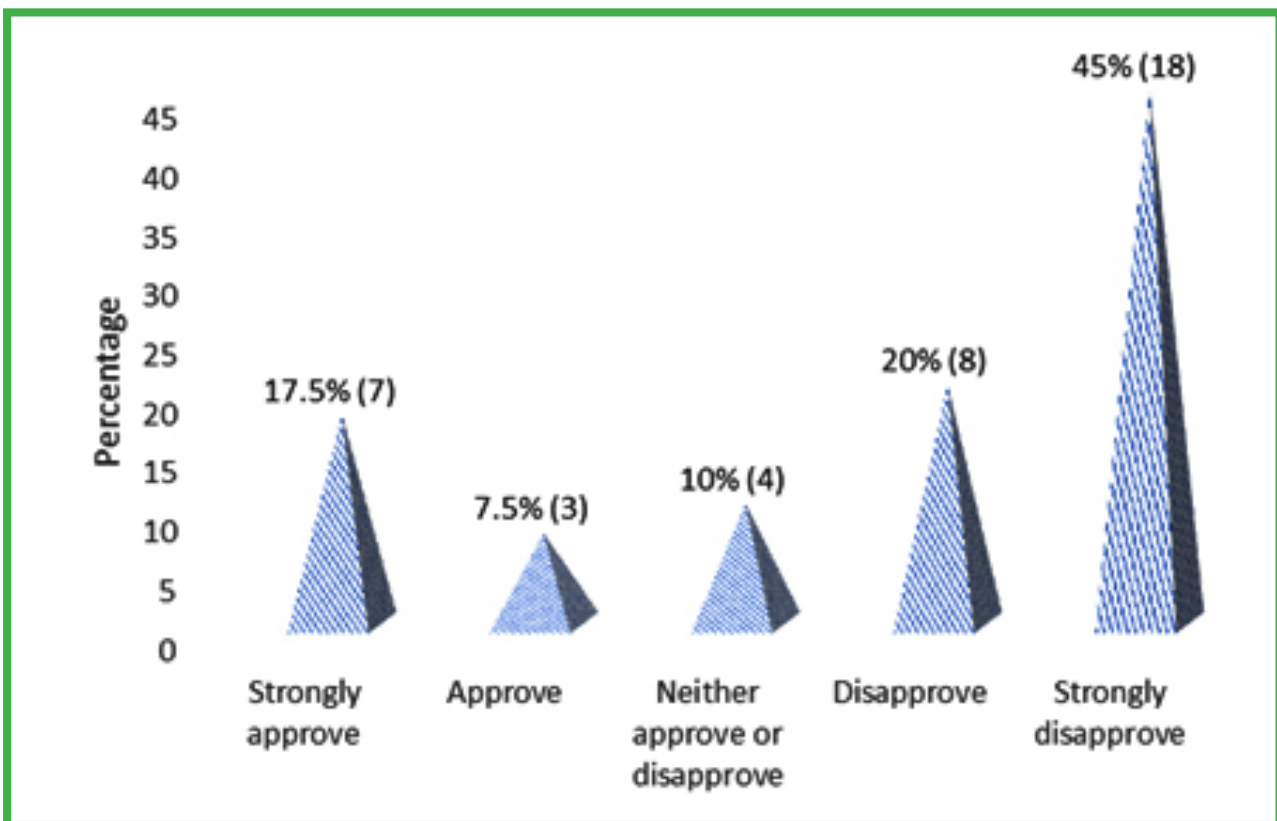


Figure 18: Proposed mandatory uses of Huduma Namba and Card when transacting with government



The above reservations concerning NIIMs and its associated Huduma Namba may have been influenced by a dominant narrative during registration process. As the government rolled out the project, concerns about the biometric identity systems were pointed out by some civil society organizations. Nubian Rights Forum- one of the CSOs most concerned with the NIIMS- argued that the identity systems could lead to exclusion, with individuals not being able to access goods and services to which they are entitled, thus potentially impacting upon other rights, including social and economic rights<sup>66</sup>. The Forum asserted that exclusion as a result of an identification system could come in two forms. Firstly, in cases where individuals who are entitled to but are not able to get an identification card or number that is used for service provision in the public and private spheres. Secondly, that even people enrolled on to biometric systems can suffer exclusion arising from biometric failure in their authentication<sup>67</sup>. The Forum also observed that data breaches associated with identity systems tend to be large in scale, with rectification either being impossible or incurring a significant cost. In addition the breaches affect individuals through identity theft or fraud, financial loss or other damage. Therefore, as the NIIMs would accommodate more data, the higher the risk.

---

<sup>66</sup>Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR, p.187

<sup>67</sup>Ibid.

# CHAPTER SIX

---

## POTENTIAL OPPORTUNITIES FOR ENHANCING AND ADVANCING DIGITAL RIGHTS IN KENYA

*This chapter presents potential opportunities for enhancing and advancing digital rights in Kenya that could be utilized by private sector, citizens, civil society organizations and government.*

### 6.1 Technology Spread and Increased Adoption of ICT in Work and Social Places

There have been many changes in the technological space in the past decade such as the convergence and integration of ICT technologies, migration from analogue to digital TV broadcasting and advancement of mobile technology enabling new services. These advancements have enabled availability of reliable and affordable digital infrastructure thereby increasing demand for technology and associated devices. This would lead to technology spread across the country which may be accompanied by clamor for digital rights.

### 6.2 Increased Participation of Private Entities

Data experts in private sector observed that there has been deliberate attempt by their organizations to make their content moderation policies better known to the public. Indeed if private entities have fair and widely known policies and implement them judiciously, it might reduce the incentive for governments to enact laws and regulations to address some of the challenges in the ICT industry. Safaricom, for instance, has been supporting initiatives that promote digital rights, while private media owners have been speaking about licensing obligations and government practices that undermine privacy and freedom of expression, protect user's data and align with initiatives that grow access, affordability and innovative use of digital technology.

### 6.3 Litigation on Digital Rights

Heightened interests in the litigation of digital rights has also opened opportunity for promotion of these rights. Like in the case of Huduma Namba case, the Nubian Right Forum, Kenya Human Rights Commission, Kenya National Commission on Human Rights, Muslims for Human Rights, Haki Centre, Law Society of Kenya and Inform Action actively challenged registration of personal data alleging that the exercise would stifle digital rights. This initiative not only contributes to safeguarding digital rights, but also more importantly, through counter-arguments in the litigation process, citizens are made aware of these rights.

### 6.4 Advocacy Work

Civil society space continues to offer additional opportunities toward informing policy making process related to digital rights. Some civil society organizations have already began conducting independent digital rights studies aimed at analyzing the legal frameworks for digital rights and making proposals that would improve the existing laws and policies. Advocacy groups such as Kenya Privacy have been keen at explaining the problem at hand and succinctly suggesting practical solutions.

### 6.5 Digital Safety and Digital Literacy

Embrace of safe digital practices and adhering to them could also promote digital rights. Poor digital security skills that are widespread on social media have been a source of blackmail and extortion from critical internet users, and in cyber bullying. Increased digital security training and digital literacy campaigns, and increased use of tools of anonymisation and circumvention would further promote digital rights. Civil society actors may leverage their networks to cooperate in building mechanisms to support at-risk activists and critical users in a coordinated, multi-faceted manner that could include physical security support, legal support, awareness raising, and digital security support.

### 6.6 Comprehensive Regulatory Framework

A comprehensive regulatory framework would operationalize the principles and standards set out in the Data Protection Act. For example, the biometric data and personal data in NIIMS shall only be processed if there is an appropriate legal framework in which sufficient safeguards are built in to protect fundamental rights. Thus far, the Ministry of Interior and National Coordination has issued the Data Protection (Civil Registration) Regulations which was subjected to public participation in February 2020 . Kenya can also borrow from India which has been hailed as one of the countries with successful regulations, the Aadhaar Act, which encompasses regulations on enrolment , update authentication, data security and sharing of information.

### 6.7 Increased Government Support

Through the Ministry of ICT, opportunities for promoting and advancing digital rights have been created through strengthening of existing institutions and assigning appropriate ICT priority areas. Opportunities to consider emerging digital rights have also been seen in developing, coordinating and implementing both the ICT policy and the monitoring and evaluation framework across all sectors of the economy to ensure that the implementation of ICT programmes and projects is effective to support the social and economic sectors of the economy.

---

Data Protection (Civil Registration) Regulations, 2020. The Regulations can be accessed at <https://ict.go.ke/wp-content/uploads/2020/02/THE-DATA-PROTECTION-CIVIL-REGISTRATION-REGULATIONS-2020.pdf>





# CHAPTER SEVEN

---

## CONCLUSION

*This study has attempted to review the history of digital rights and accompanying laws in Kenya. It also reviewed existing data rights and access to information laws in Kenya, and their implementation and analyzed the recent Huduma Namba judgment. The study further identified the perceptions of the impact of the implementation of the relevant legislation and policy proposals and identify potential opportunities for enhancing and advancing digital rights in Kenya.*

### 7.1 Summary

To recapitulate, it was highlighted that in Kenya, while the journey towards data protection and privacy gained momentum with the promulgation of the Constitution of Kenya in 2010, the history of digital rights in Kenya is intertwined with the development of Kenyan state. From colonialism to independence to post-independence era, the growth and development of digital rights and accompanying laws has taken different shades involving a complex set of organizations, actors and institutions.

Despite the evolving legal framework on digital rights and right to access to information, there are some weaknesses that potentially threaten the implementation of the rights to access information and digital rights. Although the Constitution stipulates that everyone has the right to demand any information that is in the possession of the state, the broad definition of state that includes two levels of government and their accompanying institutions places greater burden on the state than private bodies. The Access to Information Act, 2016 was enacted to operationalize and to give full legal effect to the constitutional right to access information (Article 35), and it accordingly provides broad, clear and specific on right to access information. Section 17 of the Article widens the scope of the information to include the management of records which include “documents or other sources of information compiled, recorded or stored in written form or in any other manner and includes electronic records. Similarly, the Data Protection Act, 2019 was operationalized to

give full legal effect to privacy rights, however, the government is yet to appoint Data Commissioner and it is not feasible to have data impact assessment reports done sixty days prior to processing of the data. Although the Act seeks to promote the rights of children, the rights of the child in relation to the personal data collected during minority age and upon attaining adult age are also not specified, particularly in light of their evolving capacities. As the government seeks to operationalize the Act, it has proposed Huduma Bill, yet the document has raised some concerns. There is no policy framework guiding the centralist approach in civil registration. The Bill imposes harsh sanctions for failure to register or for procuring service(s) without Huduma Namba. It criminalizes any transaction with the government if conducted without the Huduma Namba. The Bill is too heavy on technology yet it lacks adequate provisions for public education on how the technology that will be the primary anchor for the registration process operates. It also lacks provisions for enhancing informed consent in light of the digital demands of the system. The emphasis placed on the use of fingerprints to enroll or identify an enrolled person is very limiting. Given that it proposes that biometric information cannot be altered by an individual, it could be a tall order for enrolled entries in case the data is stolen or lost from NIIMS. Even before the enactment of the Data Protection Act, the government rolled out National NIIMS intended to be a single source of personal information of all Kenyans as well as foreigners resident in Kenya, an action that was opposed by some CSOs resulting to a protracted court battle.

The study collected primary data on the perceptions of the impact of the implementation of the relevant legislation and policy proposals. With regard to access to information and privacy rights the study found out that despite considerable dissatisfaction with the implementation of the Articles 31 and 35 of the Constitution, a majority of respondent were very familiar with the existence of the Acts. What is perhaps interesting is that despite dissatisfaction with implementation of the broad constitutional provisions, a majority of the respondents were generally satisfied that since the enactment of the related Acts on access to information and privacy rights there have been some positive changes. Finally, regarding NIIMS and associated Huduma Namba, it was observed that, a majority of the respondents were not sure whether the accuracy of the system would be high or low. With regard to data controls the dominant view oscillated towards the system not being so effective. As for the security of the data, a majority of the respondents did not trust that the system will secure data. Equally, a majority of the respondents did not believe that the system would be lawful, transparent and fair and still many believed that the implementation cost of the system would be too high and not sustainable. Lastly a majority of the respondents strongly disapproved the proposed mandatory uses of Huduma Namba and Card when transacting with government.

Recognizing that the above perspectives are key in instigating changes, the study is optimistic that the following opportunities can promote digital rights in Kenya: technology spread and increased adoption of ICT in work and social places; increased participation of private entities; litigation on digital rights; advocacy work; digital safety and digital literacy; regulatory framework and increased government support.

## 7.2 Emerging Issues

The current scramble for access to personal, health and general data in relation to COVID-19 has given the current research some impetus to interrogate the protection of fundamental rights and freedoms enshrined in Chapter Four on the Bill of Rights. COVID-19 data is now demanded by many organizations. Whereas many organizations are demanding the data for the management of COVID-19 and designing coping strategies aimed at flattening the curve, others are looking for the data for commercial interests or malicious purposes such as sharing of citizen status information and manipulation of information collected during the crisis. As such, this has raised a lot of concerns, that even those seeking to acquire personal data and health data for public health purpose may be using the data to undertake mass surveillance not linked to managing the crisis. Herein lies the problem with the Data Protection Act 2019. Whereas processing of data may have an impact on fundamental rights and freedoms of data subjects, the Data Protection Act provides that a data



controller must carry out a data protection impact assessment in consultation with the Data Commissioner. As pointed out, at the moment the government is yet to appoint the Data Commissioner to allow effective performance of data protection impact assessment, implying that the ongoing appropriation of personal data may potentially lead to violation of fundamental rights and freedom.

As reported in other jurisdictions like China and Russia, use of surveillance software/tools in the fight against COVID-19 poses serious threats to human rights. Given that the utility of the tools in controlling the pandemic is yet to be proven, their use for surveillance could be potentially manipulated to facilitate overreach by various States keen to spy on their citizens. Arbitrary use of unregulated surveillance software/tools has the potential of not only infringing on fundamental rights, but also assuming a life of their own even after the pandemic clears. For instance, mobile tracking programs intended to be used temporarily until the pandemic is under control may become permanent features of an expanded surveillance regime. As the mobile tracking device undermines privacy, its use may have a spillover effect on other rights, such as freedom of movement, expression, and association. The device “creates granular, real-time targeting opportunities, which can be used by governments to enforce draconian quarantine measures. This is particularly problematic in the absence of transparent and meaningful limits on data collection, retention, and use<sup>69</sup>”. What is more, over-reliance on tracking device could exclude vulnerable groups in society, thereby undermining their livelihoods and health. For instance, accuracy of contact tracing application may exclude groups such as homeless people, migrant workers and refugees staying in deplorable conditions. According to Human Rights Watch (HRW), what is important at this point is for various governments to address concerns such as reliability and validity of the tracking devices and the potential for misrepresentation of individuals’ risk of infection. Governments should also address “ways to combat the pandemic that are less intrusive on rights, including proven containment methods such as manual contact tracing and expanding access to accurate testing and treatment<sup>70</sup>”.

---

<sup>69</sup><https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks> (Accessed 25 May 2020).

<sup>70</sup>ibid.

---

## REFERENCES

---

Bierschenk, T., and Olivier De Sadan. 2009. Studying the Dynamics of African Bureaucracies: An Introduction to States at Work: Introduction', in Bierschenk, T., and Olivier De Sadan (eds), *States at Work: Dynamics of African Bureaucracies*. Leiden: Koninklijke Brill

---

Breckenridge, K.(2019). 'The failure of the 'single source of truth about Kenyans': The NDRS, collateral mysteries and the Safaricom monopoly", *African Studies*, 78:1, 91-111.

---

Brint, S, and Karabel, J. 1991. Institutional Origins and Transformation: The Case of American Community Colleges', in Powell, W. and DiMaggio, D. (eds), *New Institutionalism in Organizational Analysis*, 337 – 360. Chicago IL University of Chicago Press

---

Byrkeflot, H., Strandgaard-Pedersen, J. & Svejenova, S. 2013. From Level to Practice: The Process of Creating New Nordic Cuisine, *Journal of Culinary Science and Technology* 11, 1, 36 – 55.

---

Kivikuru, U. (2017), 'Ideals, buzzwords and true trying: ICT and communication policies in Kenya', *Journal of African Media Studies*, 9:2, pp. 307–21.

---

Kenya National ICT Master Plan 2014–2017, <http://workspace.unpan.org/sites/Internet/Documents/MoICT%20-%20Kenya%20National%20ICT%20Master%20Plan%202014%20-%202017-Lawrence%20UN.pptx.pdf>.

---

Kenya Vision, A Vision for a Competitive and Prosperous Kenya 2030, [http://thereddesk.org/sites/default/files/vision\\_2030\\_brochure\\_july\\_2007.pdf](http://thereddesk.org/sites/default/files/vision_2030_brochure_july_2007.pdf).(Accessed 19 March 2020).

---

Ministry of Information, Communications and Technology (2006), National Information and Communications Technology (ICT) Policy (2006), [http://www.ist-africa.org/home/files/Kenya ICT Policy 2006.pdf](http://www.ist-africa.org/home/files/Kenya%20ICT%20Policy%202006.pdf).(Accessed 18 March 2020).

---

— (2013), Ministerial Strategic Plan (2013–17), [www.ict.go.ke/wp-content/uploads/2016/04/MinistryStrategic.pdf](http://www.ict.go.ke/wp-content/uploads/2016/04/MinistryStrategic.pdf) (Accessed 18 March 2020).

---

Ministry of Information, Communication and Technology, 2019. National ICT Policy.

---

Ministry of Interior and Coordination of National Government, 2019. The Huduma Bill 2019.

---

Raboy, M & BD. Abramson. 1988. Grasping an enigma-cultural policy and social demand, *Cultural Studies*, 4(2):329-355.

---

Republic of Kenya, 1963. The 1963 Constitution of Kenya. Nairobi, Government Printer.

---

Republic of Kenya, 2010. The 2010 Constitution of Kenya. Nairobi, Government Printer.

---

Republic of Kenya, 2016. Access to Information Act 2016. Nairobi, Government Printer.

---



Republic of Kenya, 2018. The Computer Misuse and Cybercrimes Act, 2018. Nairobi, Government Printer.

---

Republic of Kenya, 2019. The Data Protection Act. Nairobi, Government Printer.

---

Theil, A. 2020. Biometric Identification Technologies and the Ghanaian 'Data Revolution', *Journal of Modern African Studies*, 58, 115-136.

---

Thornton, P.H., Ocasio, W., & Lounsbury, M. 2012. *The Institutional Logics Perspective: A New Approach to Culture, Structure, and Process*. New York: Oxford University Press.

---


World Bank 2013. Ghana-e-Transform Project, <http://documents.worldbank.org/curated/en/2339/1468253466632/Ghana-e-TransformProject> (Accessed 9 April 2020).

## LIST OF INTERVIEWS

No I	interviewee	Organization
1.	Paul Annan	Kenya Human Rights Commission
2.	George Kegoro	Kenya Human Rights Commission
3.	Davies Malombe	Kenya Human Rights Commission
4.	Mary Kimemia	Kenya Human Rights Commission
5.	Grace Bomu	KICTANET
6.	Victor Kimani	Kenya National Commission on Human Rights
7.	Okiya Omutata	Human Rights Activist
8.	Linda Bonyo	Lawyers Hub
9.	Rajab Muhammed	Amnesty International-Kenya
10.	Andronicus Sikula	Amnesty International- Kenya
11.	Wakesho Kililo	Lawyers Hub
12.	Mugambi Laibuta	Data Protection Expert
13.	Japheth Ondiek	Digitization Researcher
14.	Mwachofi Singo	Security Expert, UoN
15.	Ronald Simiyu	OCS, Karen Police Station
16.	Gitonga Murunga	Public Prosecutor
17.	Abdisalaam Aga Tuka	ICT Department, University of Nairobi
18.	Kevin Kimani	ICT Department, University of Nairobi
19.	Nobert Basweti	Communication Expert, University of Nairobi
20.	Herman Manyora	Communication Expert, University of Nairobi
21.	Davies Otiato	Journalist, Daily Nation
22.	Javas Miugo	Journalist, Standard Media Group
23.	Erick Oduor	Secretary General, Kenya Journalist Association
24.	Kiugu Kibara	Ministry of ICT, Youth Affairs
25.	Benson Nyagaka	Ministry of ICT, Youth Affairs
26.	Ken Odunga	Data Expert, Safaricom
27.	Rueben Thuku	Ministry of Devolution
28.	Judy Regina	County Assembly Forum
29.	Paul Mwaura	Ministry of Interior and National Coordination
30.	Alex Kosgey	Ministry of Interior and National Coordination
31.	Kennedy Ouma	Ministry of Interior and National Coordination
32.	Dan Opon	Ministry of Interior and National Coordination
33.	Pater Adika	Parliament (Senate)
34.	Kipkemboi Kirui	Parliament (National Assembly)
35.	Agnes Agade	Judiciary
36.	Esther Kimilu	Judiciary







This work was carried out in the Context of the African Digital Rights Fund with support from the collaboration on ICT Policy for East And Southern Africa (CIPESA)

supported by:



ACK Garden House  
2nd Floor, Wing A | 1st Ngong Avenue  
P. O. Box 21765, 00505 Nairobi, Kenya  
[e]: [info@mzalendo.com](mailto:info@mzalendo.com) | [w]: [www.mzalendo.com](http://www.mzalendo.com)  
[f]: [mzalendowatch](https://www.facebook.com/mzalendowatch) | [t]: [@mzalendowatch](https://twitter.com/mzalendowatch)

---

supported by Collaboration on International ICT Policy  
for East and Southern Africa.