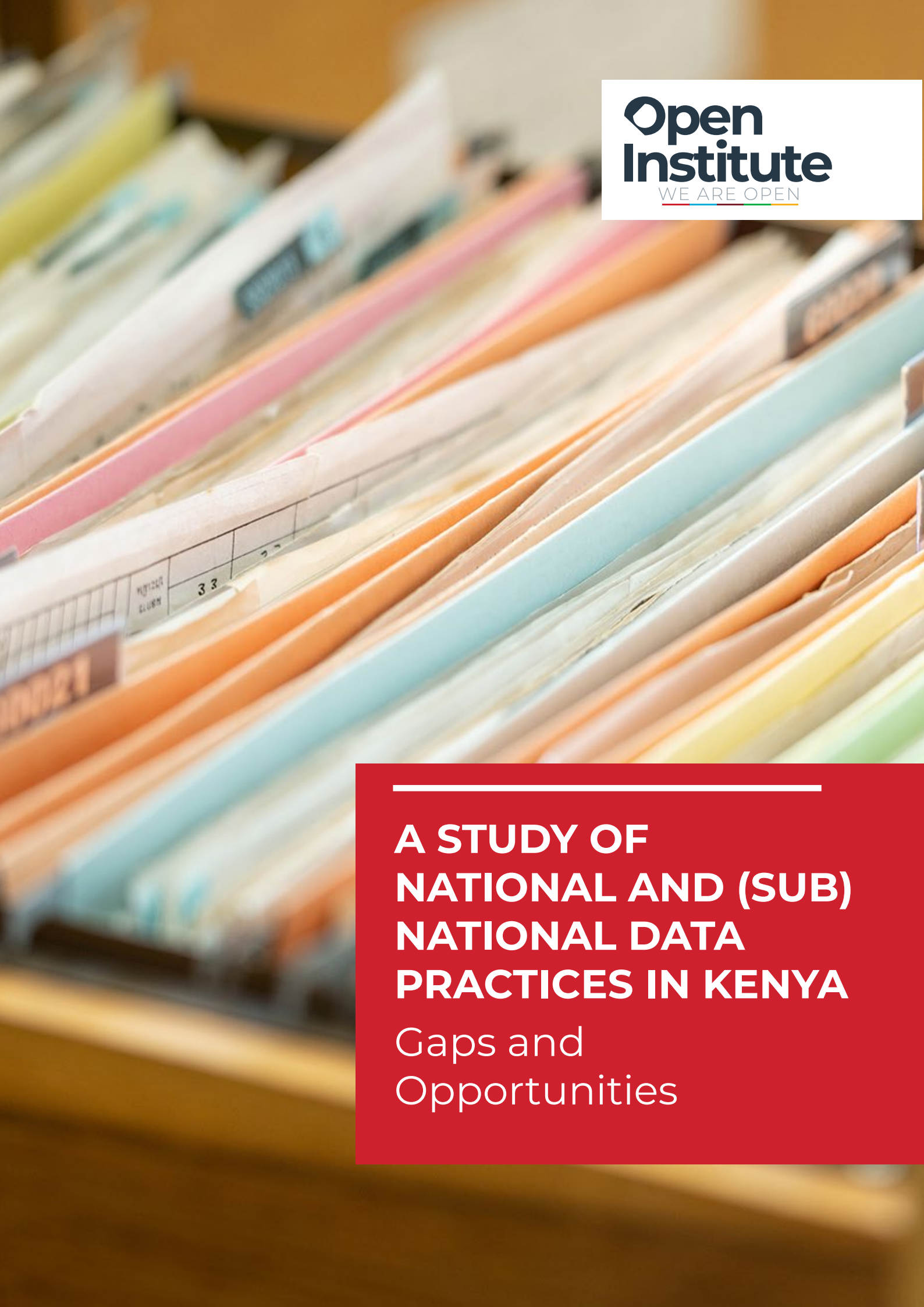


Open Institute
WE ARE OPEN

A STUDY OF NATIONAL AND (SUB) NATIONAL DATA PRACTICES IN KENYA

Gaps and Opportunities

ABOUT OPEN INSTITUTE

The Open Institute's mission is to collaborate with governments, citizens, civil society organisations and other players to develop policies, tools and knowledge that strengthen citizens' voices in the governance and development in their societies. We envision a future with an open society that is managed by informed, fact-driven citizens.

ACKNOWLEDGEMENTS

This report would not have been completed without the participation of County Officials from the County Governments of Bomet, Vihiga, Makueni, Taita Taveta and Kilifi. We also received insights from the following: Commissioner of Access to Information, Commission for Administrative Justice and the Office of the Data Protection Commissioner. Additionally, we thank all participants and respondents who heeded to our survey and participated in the focus group discussions.

Last but not least, we are grateful for input from our research consultants who were each independently instrumental for separate sections of the research.

We are grateful for all your inputs, efforts and insights.

Published by Open Institute

P.O Box 50474, Nairobi 00100, Kenya

TABLE OF CONTENTS

Abbreviations and Acronyms

ATI	Access to Information
ATIA	Access to Information Act
COK	Constitution of Kenya
DPA	Data Protection Act
DPC	Data Protection Commissioner
DPIA	Data Protection Impact Assessment
ODPC	Office of the Data Protection Commissioner

List of tables

DEFINITIONS

Data	means grouped information that is obtained, recorded, held or used in a particular way or by a particular body;
Personal Data	means any information relating to an identified or identifiable individual (data subject);
Data practice	means an aggregation of the laws, procedures and practices employed by the subnational in managing data;
Data processing	means any operation or set of operations performed on personal data such as collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetic operations on such data. The processing can be manual according to a set criterion or automated;
Controller	means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;
Processor	means the natural or legal person, public authority, service, agency or any other body which, processes data on behalf of the controller;
Recipient	means the natural or legal person, public authority, service, agency or any other body to whom data is disclosed or made available;
Subnational governments	is a term used interchangeably with county government. It means the devolved governments each comprising the county assembly and county executive. This is provided for in Article 176 of the Constitution Of Kenya (COK), 2010. In this study, subnationals (or county governments) are data controllers, processors and sometimes recipients.

1. EXECUTIVE SUMMARY

Subnational governments in Kenya have since their formation in 2013 been collecting, creating, storing, maintaining and disseminating information. The data held by subnational governments include among others budget and expenditure related data, geo-spatial data, contracting data, subscription and notification data, personal data, education data, health data (patient data), trade licences data, property approval data and law enforcement data among others.

In practice, actual data practices are guided by policy or by subjective values and influences that may vary depending on which Ministry, County, Department or Agency (MCDA) one visits. While most subnational governments in Kenya have not enacted specific Data Protection laws, they are under legal obligation to adhere to the dictates of the Constitution of Kenya, 2010, international laws applicable to Kenya and laws passed by the National Assembly on these issues.

Some of the key relevant laws are the Access to Information Act, 2016, the Data Protection Act, 2019 and the County Government Act, 2012, the Public Audit Act, 2015, the Public Finance Management Act, 2015, and the Public Service (values and Principles) Act, 2015 among others. These laws, in brief, establish rules and regulations that govern the treatment of data held by public and private bodies and the rights of data subjects.

In addition, the above laws offer different sets of opportunities for subnationals (county governments) to collect, store, maintain, process and archive both government and personal data. They also offer broad contours that must be navigated by different public officials in county assemblies, county public service boards, and county executive committees as they seek to enable citizens access to information held by them.

However, there are numerous hurdles facing subnational governments as the paradigm of government data continues to shift from highly guarded to information held in trust for the citizens. It also emanates from emerging definitions of public value that draw legitimacy from accountability and transparency which means that public managers must address the needs of citizens as well as politicians. Consequently deviating from the usual top-down models where public managers only focus on meeting centrally driven targets and performance management [1]. This "new norm" is further compounded by knowledge gaps around the government obligations on access to information and how to best balance that with the protection of the rights of data subjects. This has resulted in asymmetries which are evident in the five subnationals in this study; for starters, none have specifically deployed any data protection or information officers - with the functions spread across a number of officers as a peripheral duty.

The study was undertaken during the second and third quarter of 2021.

First, the goal of the research was to identify best practices and illuminate barriers in deployment of internationally accepted data protection principles at the subnational level. This was also undertaken in view of the opportunities and challenges offered by the Constitution of Kenya, 2010, the County Government Act 2012, the Access to Information Act 2016, and the Data Protection Act, 2019.

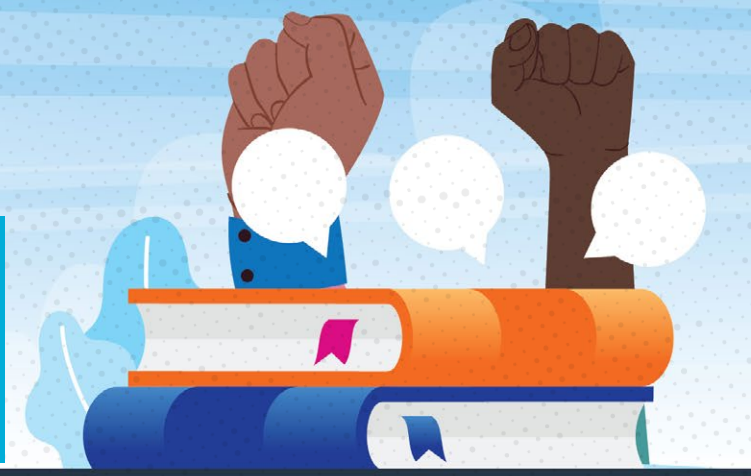
Second, this study notes that the right to privacy and the right to information are both essential human rights in the modern information society. For the most part, these two rights complement each other in data processors (both state and non-state) accountable. But there is a potential conflict between these rights when there is a demand for access to personal information held (especially by state actors). Where the two rights overlap, the government needs to develop mechanisms identifying core issues to limit conflicts and for balancing the rights.

Lastly, this study finds that indeed the Access to Information Act 2016, and the Data Protection Act 2019, offer a guide on how each of the rights may be enforced and safeguarded. However, the two laws are most of the time treated by subnationals as separate laws without drawing on their complementarity. A holistic approach by both national and county governments will ensure we tap on the complementarity of the laws. In this report, this is posited through the use of the concept of information rights (depicted further in the recommendations of this report).

2

BACKGROUND

Information Rights



First, information rights are fully entrenched in the Constitution of Kenya, 2010 (herewith 'the Constitution'). In this study, we use information rights to refer to privacy,[2] expression[3] and access rights.[4] These three rights have a bearing on active citizenship, public participation and efforts to ensure accountable use of data obtained from citizens. Further, the constitutional provisions on public participation is a key pillar that has an impact on realisation of information rights. We draw on Murdock in his use of the concept of information rights to mean "comprehensive and disinterested information about current events and conditions and about the actions, motives and plans of all those institutions-both government and corporate-with significant power over their life chances and living conditions."[5]

Second, the predominance of the values and principles which demand the participation of citizens in the governance of the country permeate the Constitution, and more prominently articulated in Articles 10, 118 and 119 of the Constitution, which require state agencies to facilitate public participation. Within the context of devolved governance which Kenya adopted as part of its constitutional governance structure, the County Government's Act (2012) further entrenches the participation of citizens in the governance of the counties. In particular, Section 87 of the Act provides for the following principles of public participation in the counties:[6]

1. Reasonable balance in the roles and obligations of county government and non-state actors in decision-making processes to promote shared responsibility and partnership and to provide complementary authority and oversight;
2. Timely access to information, data, documents, and other information relevant or related to policy formulation and implementation;
3. Reasonable access by citizenry to the process of formulating and implementing policies, laws, and regulations, including the approval of development proposals, projects, and budgets, the granting of permits, and the establishment of specific performance standards;
4. Protection and promotion of the interest and rights of minorities, marginalized groups, and communities and their access to relevant information;
5. Legal standing for interested or affected persons, organizations, and where pertinent, communities to appeal from or review decisions or redress grievances with particular emphasis on persons and traditionally marginalized communities, including women, the youth, and disadvantaged communities.
6. Promotion of public-private partnerships, such as joint committees, technical teams, and citizen commissions, to encourage direct dialogue and concerted action on sustainable development, and;
7. Recognition and promotion of the reciprocal roles of non-state actors' participation and governmental facilitation and oversight.

Lastly, the right to access information and the right to data protection (the right to privacy) are essential parts of the protection of human dignity in modern democratic information societies.[7] The two rights are also facilitative in the protection, promotion and fulfilment of a set of other rights among them right to education and right to health.[8] For the most part, as discussed in the introduction of this report, these two rights complement each other in assisting citizens hold their governments accountable. The Constitution and a set of supporting legislative instruments oblige County Governments in Kenya to have an obligation to ensure the realisation of these rights.

Access to Information

First, in 2016 Kenya passed the Access to Information Act, 2016 in fulfilment of its obligations under the constitution Article 10, Article 33 and 35. There has been limited progress in implementation including training of public officials on their obligations under the law, appointment or designation of information officers in most MCDA's. However, lack of regulations has hampered its effective implementation. The Commission on Administrative Justice (CAJ), the oversight mechanism under the Access to Information law, has also not filed annual reports to the National Assembly as required by law (during the period from 2016). Consequently, there is no report yet to enable an assessment on the state of access to information in Kenya.[9]

In addition, Kenya is one of the 78 national signatories to the Open Government Partnership (OGP) and has been since 2011. Presently, the country is implementing the Fourth National Action Plan with clear commitments around beneficial ownership and open contracting[10]. A number of subnations are signatories namely: Elgeyo Marakwet, Nairobi, Makueni and more recently Nandi. Makueni is the only subnational in the study that is already a member of the OGP. It joined in 2020.[11] A comment here suffices, there is a need to address the issue of sustainability and resilience of Kenya's OGP agenda as interest seems to vary from successive governments.[12]

As a practical example of asymmetry, non-state respondents from Kilifi, Vihiga and Taita Taveta indicated that they would have preferred to get more information on tenders and county government expenditures - but these are not readily available.

Second, the Commission on Administrative Justice (CAJ) has developed and issued a model law on access to information for county government,[13] and engaged a number of subnationals to encourage them to enact their specific access to information laws. Kilifi and Makueni are two of the study subnationals that the CAJ has directly engaged with on this issue.[14] Through the engagement with subnational governments, CAJ indicated 46 of the 47 subnational have made appointments and designated access to information officers.[15]

Further, CAJ reports (reported to this study through the Commissioner of Access to Justice) has so far received 369 applications for review and appeals on refusal to disclose information and that they have effectively resolved 332 applications (89.9 per cent). They have issued 30 enforcement orders requiring various public bodies to disclose certain sets of information to the requesters; three are pending before the High Court. The Commission has trained 7904 public officials across the country on their legal obligations under the Access to Information Act, 2016 in the last five financial years.

Third, through collaboration with civil society organisations, CAJ has finally developed the Access to Information (General) Regulations, 2021,[16] and is in the process of engaging the Ministry of ICT and other relevant stakeholders to ensure they are gazetted and operationalised.

We also note that there are three important legal documents at the international level that obligate states to guarantee the right to information for citizens. These international instruments have been critical to interpretation of the right to information in Kenya even before enactment of the Access to Information Act 2016.

Kenya has ratified three of them (with the exception of the African Union Convention on Cyber Security and Personal Data Protection). These include:

Universal Declaration of Human Rights (UDHR)[17], Article 19:

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

By virtue of its membership in the UN, Kenya is obligated to adhere to the principles of the UDHR.[18]

International Covenant on Civil and Political Rights(ICCPR)[19] , Article 17:

"...2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.. ."

Kenya acceded to the ICCPR on 1st May 1972.[20]

Going a step further to safeguard the right to information, the Human Rights Committee adopted General Comment 34 of 2011[21] . The Comment expounds on Article 19 of the ICCPR.

States ought to make a report of every law that allows for the interference with the right to information. The reports must also include all complaints on any arbitrary or unlawful interference with the right to information.

African Charter on Human and People's Rights (ACHPR), Article 9[22]

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

Kenya acceded to the ACHPR on 23 January 1992.[23]

Data Protection and Privacy

First, Kenya enacted its Data Protection Act in November 2019 to regulate the processing of personal data, and provide for various rights and remedies to data subjects residing in Kenya. The act establishes the Office of the Data Protection Commissioner (ODPC) as the national data protection authority to oversee the implementation of the Act. In November 2020, the first Data Protection Commissioner Ms. Immaculate Kassait was sworn into office, and has since worked on operationalizing and implementing the Act. Her office has currently released draft regulations which are undergoing public participation.[24]

Second, the researchers note that Kenya's philosophy on privacy is informed by Kenya's participation in the international community. The Kenyan Data Protection Act bears some similarity with the EU General Data Protection Regulation (GDPR)[25] and if properly implemented it may be a step closer to achieve adequacy status from the EU. We also note that there are four important legal documents at the international level that obligate states to guarantee data protection and privacy rights to citizens. These international instruments have been critical to interpretation of the right to privacy in Kenya even before enactment of the Data Protection Act 2019.

Kenya has ratified three of them (with the exception of the African Union Convention on Cyber Security and Personal Data Protection). These include:

Universal Declaration of Human Rights (UDHR)[26] , Article 12

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

By virtue of its membership in the UN, Kenya is obligated to adhere to the principles of the UDHR.[27]

International Covenant on Civil and Political Rights(ICCPR)[28], Article 17

"...1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks..."

Kenya acceded to the ICCPR on 1st May 1972. [29]

Going a step further to safeguard the right to privacy, the Human Rights Committee adopted General Comment 16 of 1988[30]. The Comment expounds on Article 17 of the ICCPR to provide for:

a. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Likewise, any interference with the right to privacy must be grounded in law and must be reasonable.

b. Secondly, every individual has the right to ascertain in an intelligible form, whether their personal data is stored in automatic data files, and if so, for what purposes and by which public or private entity or person.

c. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

d. States ought to make a report of every law that allows for the interference with the right to privacy. The reports must also include all complaints on any arbitrary or unlawful interference with the right to privacy.

African Charter on Human and People's Rights (ACHPR)[31]

First, while the African Charter on Human and Peoples' Rights does not explicitly guarantee the right to privacy, it may be inferred from several Articles relating to the integrity of the person, the right to dignity and the right to property. There has been much debate as to whether the right to property is best placed to safeguard personal data of an individual and realize their right to data protection. In the EU, the law safeguards personal data as a right different from the right to property however, the right to property has been used to protect property interest in databases[32]. In other jurisdictions, personal data may be treated as valuable property of the data subject that they can exchange for monetary compensation or grant permission for others to use .[33]

Article 4: "...Human beings are inviolable. Every human being shall be entitled to respect for his life and the integrity of his person. No one may be arbitrarily deprived of this right..."

Article 5: "...Every individual shall have the right to the respect of the dignity inherent in a human being and to the recognition of his legal status. All forms of exploitation and degradation of man, particularly slavery, slave trade, torture, cruel, inhuman or degrading punishment and treatment shall be prohibited..."

Article 14: "...The right to property shall be guaranteed. It may only be encroached upon in the interest of public need or in the general interest of the community and in accordance with the provisions of appropriate laws..."

Kenya acceded to the ACHPR on 23 January 1992 .[34]

African Union Convention on Cyber Security and Personal Data Protection[35]

First, the African Convention is not yet a legally binding document but is persuasive given it was drafted and approved by all African Justice and ICT Ministers prior to presentation before the African Heads of States for ratification and domestication. The right to privacy is protected under Article 8 (Objective of this Convention with respect to personal data) and highlights that the entire convention is governed by the "***principle of free flow of personal data" ,*** Article 10 (Preliminary personal data processing formalities), Article 13 and 14 (Specific principles for the processing of sensitive data), and Article 25 (Legal measures).

Specifically, the researchers note that Article 13 and 14 lists the following principles:

1. Principle 1: Principle of consent and legitimacy of personal data processing
2. Principle 2: Principle of lawfulness and fairness of personal data processing
3. Principle 3: Principle of purpose, relevance and storage of processed personal data
4. Principle 4: Principle of accuracy of personal data
5. Principle 5: Principle of transparency of personal data processing
6. Principle 6: Principle of confidentiality and security of personal data processing

Kenya has not ratified this convention, in fact only 8 countries in Africa have ratified this convention which has slowed down the coming into force of the convention.[36]

International Resolutions and Standards on Access to Information and the Right to Privacy

Additionally, there are 11 critical instruments at the international level that provide principles that states should consider in order to facilitate access to information and the right to privacy rights of Kenyan citizens. All these principles are applied globally and implement Article 12 and Article 19 of the Universal Declaration of Human Rights (UDHR). These principles are not binding but the researchers note that courts have relied on these principles especially before enactment of the 2019 Data Protection Act and the 2016 Access to Information Act. These include:

African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa[37]

The Declaration was drafted by the African Commission on Human and People's Rights in 2019 and replaces a previous 2002 version. The declaration has 43 principles and outlines the linkages between freedom of expression, access to information and the rights to privacy in Africa.

United Nations Guiding Principles on Business and Human Rights[38]

The Guiding Principles were drafted by the United Nations in 2011 and outlines bare minimums on the interaction of Businesses and Human Rights. The Principles are divided into three sections which include: the state duty to protect human rights, the corporate responsibilities to respect human rights and access to remedy. These principles provide a framework for businesses to enable access to information and promote the respect of the right to privacy.

Ten (10) Internet Rights and Principles by the Internet Rights and Principles Dynamic Coalition[39]

The Internet Rights and Principles Dynamic Coalition is a global dynamic coalition under the United Nations Internet Governance Forum. Under Principle 2 and Principle 5, the ten (10) Internet Rights and Principles state that everyone shall have equal right to access to a secure and open internet and the right to privacy on the Internet including freedom from surveillance, the right to use encryption and the right to operate anonymously.

Tunis Agenda for the Information Society (World Summit on the Information Society-WSIS)[40]

The World Summit on the Information Society (WSIS) was a two phase United Nations Conference focused on Information, Communication and technology and under paragraphs 26, 27 42 and 46; the outcome document referred to as the Tunis Agenda calls for measures to ensure access to the internet and the respect of Internet users' privacy and the protection of personal information and data. Kenya as a country participated in the WSIS phases through delegations from the Ministry of Foreign Affairs, Communications Regulator and the ICT ministry and thus the outcome is also applicable to Kenya.

Seoul Declaration for the Future of the Internet Economy (OECD)[41]

Under pp. 4, p.8, p. 9 and p. 10 of the Seoul Declaration; it calls for enabling new forms of civic engagement and participation that promote seamless access to communication and information networks, privacy and for protection of digital identities, personal data as well as the privacy of individuals online including under circumstances of cross-border co-operation of governments and enforcement authorities. Kenya as a country regularly participates in various OECD initiatives including signing some documents pushing against offshore tax evasion and avoidance[42] . Given that enforcement of this document would necessitate sharing of personal data, it is important to note this document as part of soft power.

NETmundial Multistakeholder Statement (Conference Outcome)[43]

NETmundial was a global multi stakeholder conference held in 2014 and produced outcomes and principles for internet governance. Under the document's first Internet Governance Principle (Human Rights and Shared Values) it calls for:

"Privacy: The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data.

The right to the protection of the law against such interference should be ensured.

Procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, should be reviewed, with a view to upholding the right to privacy by ensuring the full and effective implementation of all obligations under international human rights law.

Freedom of information and access to information: Everyone should have the right to access, share, create and distribute information on the Internet, consistent with the rights of authors and creators as established in law."

UN Human Rights Council (HRC) resolution on "the right to privacy in the digital age"

On March 23, 2017, the resolution on "the right to privacy in the digital age" (A/HRC/34/L.7/Rev.11[44]) was adopted by consensus at the 34th Session of the UN Human Rights Council (HRC). The resolution was led and supported by 72 UN member States.

The resolution reaffirmed the office of the United Nations Special Rapporteur on Privacy. The 2017 resolution builds upon one previous UNHRC resolution and decision and three UN General Assembly resolutions of the same title, all as a result of the global debate provoked by Edward Snowden's revelations in 2013 (captured in his 2019 autobiography 'Permanent Record') on the human rights implications of States' mass surveillance practices.

The significance of the 2017 resolution is that for the first time, the UNHRC stated that:

"States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality"

Additionally, for the first time the 2017 resolution emphasises that technical solutions to secure the confidentiality of digital communications, including measures for encryption and anonymity, are important for all people's enjoyment of human rights, including freedom of expression, and that States must not interfere with the use of such technical solutions. This expands on the HRC's affirmation of this principle in relation to journalists and the protection of their sources[45] in 2016, and aligns with the recommendations of the UN Special Rapporteur on the right to freedom of expression[46] .

Resolution 362 of The African Commission on Human and Peoples' Rights (ACHPR)[47]

In November 2016, the ACHPR passed resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa. The resolution recognized that access to information online and privacy online are both important for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.

The African Declaration on Internet Rights and Freedoms[48]

In 2014, together with Global Partners Digital, the Association for Progressive Communications (APC), the Media Rights Agenda (MRA) and around 20 organizations, ARTICLE 19 Eastern Africa reviewed and led the advocacy process that saw the African Commission on Human and Peoples Rights (ACHPR) adopt the African Declaration on Internet Rights and Freedoms (ADIRF).

Article 4 states: "...**4. Right To Information-** ***Everyone has the right to access information on the Internet. All information, including scientific and social research, produced with the support of public funds, should be freely available to all, including on the Internet ...."***

Article 8 states:"...8. **Privacy And Personal Data Protection-** ***Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.***

The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim..."

International Principles on the Applications of Human Rights to Communications Surveillance (Necessary and Proportionate Principles)[49]

In 2014, a coalition of civil society organisations (CSOs) including the Electronic Frontier Foundation, Privacy International, Access Now, and ARTICLE 19 led the development of 13 principles that set minimum standards for the protection of the rights to freedom of expression and privacy in the age of mass surveillance. They have now been endorsed by over 258 CSOs around the world and cited by others such as the United Nations Special Rapporteur on Freedom of Expression and Opinion[50] , the United Nations High Commissioner for Human Rights[51] , European Parliament[52] and European Commission[53]

Global Principles on Freedom of Expression and Privacy[54]

In 2017, ARTICLE 19 published the standard setting "Global Principles on Freedom of Expression and Privacy", a ground-breaking document which provides a comprehensive, updated framework on the mutually reinforcing nature of these two rights in the digital world. The Principles are based on international law and best practices from around the world, as reflected, inter alia, in national laws and the judgments of national courts.

While the implementation of both Access to Information and the Data Protection laws offer a number of opportunities for entrenching the principles of public participation, accountability and transparency, their potential has not been fully felt thanks to different challenges. These are highlighted in the next section of this report.

Complementarity and Conflict in Access to Information and Data Protection Laws

Inevitably, there are overlaps in access to information and privacy interests that can lead to conflicts. Sub-national governments collect large amounts of personal information, and sometimes there is a demand to access that information for various reasons. The requesters range from civil society groups advocating for accountability and transparency; investigative journalists, individuals demanding to know why a decision was made in a certain way, companies seeking information for marketing purposes or for purposes of winning tenders, and historians and academics researching recent and past events.

Over the next decade, Kenya hopes to achieve its development objectives by harnessing the benefits of the digital economy, this is documented in Kenya's Digital Economy Blueprint as a key step to diversification and development of the Kenyan Economy[55] . In 2019, Kenya published a report highlighting the potential public benefits of exploiting distributed ledger technology and Artificial intelligence.[56] Further, the country's Digital economy blueprint aims to have a digitally empowered citizenry living in a digital society. It recognises having a digital government as a key pillar to achieving this goal by realizing open data sources, digital identity for all, digital service delivery and an e-government. [57]

Undoubtedly, a digital government is able to derive high quality data that would guide decision and policy making. The World Bank recognizes the potential of exploiting data for development to improve lives by addressing poverty, managing public debt and the prudent allocation of scarce natural resources.[58] They further recognize the benefits of data sharing among both public and private entities in realizing this goal. Kenya has a devolved system of government consisting of 47 counties at subnational level. The potential to use data to inform the allocation of resources and economic development meets the objectives of devolution under the Kenyan constitution to promote social and economic development and the provision of proximate easily accessible services throughout Kenya.[59]

Open data and digital government would also facilitate civic participation and public accountability. The Constitution of Kenya, 2010 changed the governance landscape in Kenya by recognizing public participation, transparency and accountability as important national values and principles of governance. Nevertheless, meaningful and effective public participation can only be achieved with access to the right information. Therefore, citizens have a right to access data held by public authorities in the enforcement of their rights.

Despite these benefits, personal data must still be protected and the right to privacy respected. States must also guard against data misuse and abuse by creating strong data governance mechanisms that protect personal data, reinforce the right to privacy and build trust and confidence among citizenry.

Ideally, comprehensive data protection and privacy laws ought to safeguard the integrity of data that has been collected by both state and non-state actors to ensure that it is only used for the purposes for which it was collected, stored and processed appropriately. This is particularly important considering the fact that the data collected is usually of personal nature and if misused could have dire consequences to citizens and rightful delivery of service by both state and non-state actors.

Right to information (RTI) and privacy laws can both complement and conflict with each other, depending on the situation. Only in a small number of cases do they overlap and lead to potential conflict.

In many countries, Kenya included, the two rights are intertwined constitutionally. Under the concept of habeas data- a constitutional right that permits individuals to demand access to their own information and to control its use. For instance, Article 35 (2) of the COK, 2010 provides that "every person has the right to the correction or deletion of untrue or misleading information that affects the person."

"The right to obtain personal information contained in public or private databases, has been important in many countries in exacting accountability for human rights abuses and helping countries scarred by human rights abuses reconcile and move forward, which can only be accomplished by exposing the truth and punishing the guilty."[60]

In many cases, the rights overlap in a complementary manner. Both rights provide an individual access to his or her own personal information from government bodies, data protection laws allow for access to personal information held by both public and private bodies. In this study, the government bodies of interest are the subnationals.

From the above, the Access to Information (ATI) Act, 2016 and the Data Protection Act, 2019 also mutually enhance each other: privacy laws are used to obtain policy information in the absence of an ATI law, and ATI laws are used to enhance privacy and data protection by revealing abuses[61]

Thus, there are four main commonalities between Access to Information and Data Protection laws. First, the most obvious commonality between the two types of laws is the right of individuals to obtain information about themselves that is held by government bodies. This access is an important safeguard to ensure that individuals are being treated fairly by government bodies and that the information kept is accurate.

In Kenya, a country with both the Access to Information Act, 2016 and the Data Protection Act, 2019, the general approach is to apply the latter to individuals' requests for personal information;[62] requests for information that contains personal data about other parties are handled under the Access to Information Act.[63] However, this general approach does not preclude applications made under both laws by individuals for their own personal information or where such individuals want such information corrected or deleted.[64]

The second commonality between Access to Information and Data Protections laws is where the latter provide an important complement to ATI provisions by extending individuals' right of access to private bodies. Over 25 countries in Africa have passed Data Protection laws that apply to private bodies as well as government bodies. These laws give individuals the right to obtain personal information from private bodies. The use of laws may reveal abuses by corporations or other private bodies such as malfeasance by banks, political parties,[65] digital lenders,[66] ICT companies, hotels and previous employers.

The third commonality between the access to information and data protection laws is that the latter can be used to obtain policy information.[67] Journalists and media outlets, in some countries, have also used Data Protection laws to discover that officials have been spying on their phone records to discover their sources of information.[68] Similarly, ordinary citizens have used the laws to discover that the media has been intrusive.[69]

The fourth commonality is that in many countries, ATI laws are a primary tool used by privacy advocates to identify abuses and to campaign effectively against them. For example, in the United States, groups such as American Civil Liberties Union, the Electronic Frontier Foundation routinely use the USA Freedom of Information Act and state laws to demand government records on new and existing government programmes (communications surveillance, body scanners, and spying on groups) and use the records to campaign against those programmes and proposals.[70] In Kenya, the National Coalition on Human Rights Defenders has used the law to find out more information on surveillance systems.[71]

3

ABOUT THIS STUDY

First, this study examined the perceptions and experiences of citizens and government officials with regard to citizens' access to information and data protection. Despite the fact that citizens have the right to access information in exercise of their right to public participation, these rights occur in tandem alongside the right to privacy and be compliant with data protection legislation. Additionally, while using data for development presents numerous opportunities, this too must conform to data protection principles and legislation.

Second, while the ODPC continues to implement the Data Protection Act 2019, there is a need to examine policy and practices at subnational level that impact the implementation of this legislation. Further, this must be balanced against established policies that promote public accountability in areas like finance. We must also determine the role of other non-state actors at the subnational level to implement the legislation as compared to the Access to Information obligations. Therefore, this report will draw recommendations from a comparative study of 5 counties on best policy approaches to solve the aforementioned problem.

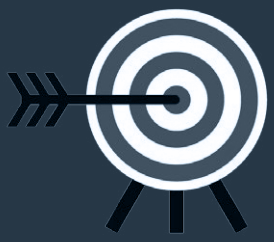
Third, in detail, the report looks into answering the following questions based on the terms of reference for the research:

1. What are the opportunities and challenges presented by legislation that encourages access to information and public participation against compliance with the Data Protection Act 2019?
2. What are the subnational policies and practices that promote access to information and Data protection while emphasizing on policy making processes and enhancing public accountability?
3. What are the requisite human resource capacities and skills required at subnational level for the implementation of the data protection Act?
4. What roles could non-state actors at subnational level play in actualizing the data protection Act 2019?
5. How best could we implement the data protection Act in a manner that promotes data governance and responsible use of data at subnational level?

The overall objective of the study

To examine policy and practices gap analysis for the main challenges and opportunities for actualisation of Kenya's Access to information Act, 2016 and Kenya's Data Protection Act, 2019 and at the select counties.

The Specific objectives investigated in this study were fourfold:



1. Juxtapose the opportunities and challenges presented by the Constitution of Kenya 2010, Access to Information Act, 2016 and the County Government Act, 2012 which uphold public participation against the Data Protection Act (DPA), 2019;
2. Analyse subnational policies and practices that promote Access to Information and Data Protection with emphasis on policy making processes and instruments as well as how public accountability is enhanced;
3. Provide policy recommendations and good practices that promote data governance and responsible use of data at subnational level.
4. Examine requisite human resources capacity and skills required at the subnational level for the implementation of the DPA;

Fifth, the study covered five counties, namely: Makueni, Vihiga, Kilifi, Bomet and Taita Taveta. Interviews were held with citizens and county government officials. The interview tools utilized were a structured survey questionnaire with county government officials, and focus group discussions with citizens.

Lastly, the remaining sections of the report are organised as follows: a methodological section, the findings section and, the conclusion section.

4

METHODOLOGY

First, mixed methods employing both qualitative and quantitative methods were used in collecting, analysing and interpreting data. The predominant method employed was qualitative – where the study employed a purposive sample of a series of informant interviews that included inquiry, reflection and meaning making of actual practices on the ground.[72]

Second, an extensive desktop research was also undertaken to not just identify applicable legal instruments but also review cases that may be of interest that have occured in the past with a view to understand what is legal, feasible, permissible and acceptable.

Lastly, the team of researchers visited each county and conducted key informant interviews with county government officials and focused-group discussions with purposefully sampled citizens. In total the study reached 58 respondents which was 77.3 percent of the respondents targeted. The collection of data occurred in Kilifi, Taita Taveta, Bomet, Makueni (with delays on the final data collection in Makueni county impacting the final analysis and presentation of results) and Vihiga counties.

5

SCOPE OF STUDY

The study limited itself to an in depth look at national and subnational data practices (by focusing on five subnationals) in Kenya. It was conducted between 5th July – 20th August 2021. The study's findings are aimed at creating a better understanding of the current practices and laws that enable data protection and data rights. It is in understanding these realities and in line with the objectives that asymmetries can be identified and sound recommendations made.

By comparing approaches used in each county, the study sought to establish the extent to which localized prevailing norms and practices of governance; the ideas, beliefs and attitudes of key actors; and their power and influence/ positions shape the interpretation and the procedural application of the law. The study is also qualitative, that is, it also seeks to explain realities that may be subjective, tentative, emergent and contextually derived.[73]

In terms of sampling, Kenya has 47 counties established under Article 176 (1) of the Constitution of Kenya. Different political parties won the gubernatorial seats.[74] The composition of the leadership of the counties and the county assemblies vary remarkably. The legislative composition plays a vital role in the county assemblies' processes of drafting, introducing bills, discussing, formulating laws, drafting regulations and formulating the policies. The structures are symmetrical to national politics many a time where party representations tend to reflect on regional popularity of big political parties in the country. We purposefully sample 5 counties for the study. The counties are Bomet, Kilifi, Makueni, Taita Taveta, and Vihiga.

The five counties selected are largely rural. Taita Taveta is a transport corridor. Bomet, Taita Taveta and Vihiga have first term governors while those of Makueni and Kilifi are serving their second and final terms in office. In terms of governors approval rating, the highest of the five is Makueni at 74.4 and the lowest is Taita Taveta at 44.6 per cent.[75]

Table 1: Source : Infotrak, Countytrak by Regions

County	Approval rating of governor	Term of the Governor
Makueni	74.4%	Second
Bomet	60.6%	First
Vihiga	60.5%	First
Kilifi	56.9%	Second
Taita Taveta	44.6%	First

This rating is important as it could be an indicator on laws and policies proposed by the county executive. A county governor with a high approval rating is more likely to be a result of greater transparency and accountability or vice versa and therefore greater responsibilities and budget. [76]

Table 2: Adapted from IEBC election report

County	Number of MCAs	Elected MCA	Nominated MCA
1. Vihiga	38	25	13
2. Taita Taveta	33	20	13
3. Makueni	48	30	18
4. Kilifi	53	35	18
5. Bomet	36	25	11

The composition of the select county assemblies is equally important. This is because pursuant to Article 185 of , county assemblies have legislative power. They have power to make or amend county laws and also oversight the county executive. For this study, we make two assumptions. First, any county assembly with a single dominant ruling party could use their numbers to block policies and laws that entrench accountability and transparency. Second, a county assembly with no single dominant party could be more likely to pass laws and policies that entrench accountability and transparency.

In Kilifi, 77.14 per cent of Members of County Assembly (MCAS) are drawn from the Orange Democratic Movement (ODM). The party also enjoys a majority of 40 per cent in Taita Taveta county assembly.

Makueni is dominated by the Wiper Democratic Movement-Kenya (WDM-Kenya)- (43.9%). Bomet county assembly is dominated by the Jubilee party (88%) and Vihiga county assembly is dominated by Amani National Congress (42 per cent).

According to Infotrak, of the five study subnationals, Makueni had the highest consolidated MCA's rating in 2020 at 54.2 percent (see table below for the approval of other leaders per county)[77]. The MCAs rating brings together the average performance of all members such that in the eyes of their electorate, they can be described as performers or non-performers depending on their score ratings. The average is the sum total of the score of each of the MCA divided by the number of MCAs per county assembly.

Table 3: Adapted from Infotrak study County Ratings 2020

	Makueni	Taita Taveta	Vihiga	Bomet	Kilifi
Governor	79.4	44.6	60.5	60.6	56.9
Senator	66.4	47.6	50.7	47.5	46.6
Women Rep	54.0	46.3	43.4	47.2	46.5
MCAs	54.2	47.6	51.1	48.3	50.2

International Budget Partnership's (IBP) Open Budget Survey reports assessed a country in three main areas namely: transparency, public participation, and budget oversight. IBP measured public access to information on how the central government raises and spends public resources. It also assessed online availability, timeliness, and comprehensiveness of eight key budget documents using 109 equally weighted indicators and scored each country on a scale of 0-100. A transparency score of 61 or above indicates a country is likely publishing enough material to support informed debate on the budget.[78] In 2019, Kenya had a transparency score of 50 (out of 100) and was ranked 49 out of 117 countries studied.[79]

According to IBP Kenya County Budget Transparency Survey, the 47 subnationals can be categorised into five groups according to their performance on how readily they disclose budget related information. The categories are: A(81-100); B(61-80); C(41-60); D(21-40); and E (0-20). The survey finds that the average transparency score across Kenya's 47 subnationals is 33 out of 100 points. This means that counties are not making budget information available to the public and are not disclosing the kind of information that, by law, counties are required to provide to the citizens and civil society to perform the oversight roles. The score varies from 73 to zero, with West Pokot County providing the highest level of information in budget documents relative to other counties.

Among the five subnational in this study, Makueni scores the highest in terms of availability of budget information. The other four scored poorly with Taita Taveta scoring a zero as seen in the table below. Taita Taveta scores zero because it did not provide any information at all nor publish any of the eleven budget documents evaluated during the survey.

Table 4: Adapted from IBP Kenya County Budget Transparency survey 2020

County	Budget information accessibility and transparency
Makueni	70%
Vihiga	47%
Kilifi	30%
Bomet	10%
Taita Taveta	0

The Special Audit on the utilization of COVID-19 funds by county governments also provides insights and understanding of how the counties deal with the good governance imperatives including transparency and the data protection obligations. The audits conducted and published pursuant to Section 32 of the Public Audit Act, 2015, helped the study underscore the issue that there is an accountability challenge and transparency deficit. As such, access to budget and public procurement-related information from all the subnationals in the study remains problematic. All the five counties selected for this study have challenges on audit issues as raised by the Office of the Auditor-General.[80]

The audit, in general, identified various irregularities including lack of approved budgets (Makueni, Kilifi and Bomet); irregular splitting of contract for supply, delivery and installation and commissioning of COVID-19 isolation wards (Bomet), supplies that were never received (Bomet) and failure to value and disclose donations in their books of account (Kilifi, Bomet, Makueni, Vihiga, Taita Taveta).[81]

The Special Audit established that the County Government of Bomet had in place a work plan, procurement plan, training plan and approved budget for the County Emergency Fund financed from its own source and the Conditional Grant received from the National Government, there were glaring issues of concern in that there was no evidence of existence of approved budgets for DANIDA funds (Kshs.6,615,000) and Frontline Healthcare Workers Allowances (Kshs. 31,470,000). While all counties received funding from Danida and allocation for Frontline Healthcare workers, Bomet was highlighted in the audit for not having sought budget approval from the county assembly.

Lastly, lack of access to timely and comprehensive information denies citizens credible tools to use to contribute effectively to policy discussions and holding those in public office accountable. Information asymmetry then becomes a tool used by those in public office to ensure there is no meaningful and well- informed citizen engagement and oversight by county assemblies and independent audit institutions.

6

FINDINGS

National Level

The Constitution of Kenya 2010

First, the Constitution of Kenya is its supreme national law and binds all persons and all state organs. Kenya is party to several international legal instruments that provide for the right of access to information by dint of Article 2(6) of the Constitution.[82] The right to access to information has been internationally affirmed under the Universal Declaration of Human Rights (UDHR)[83] as well as the International Covenant on Civil and Political Rights[84] (hereinafter the 'ICCPR') which Kenya has both ratified.

Similarly, the right to privacy which goes hand in hand with data protection is also expressly provide for in both the UDHR[85] and the ICCPR[86] as espoused in the introduction. Ratification of these legal instruments imposes a positive obligation on the state to ensure that these rights are accessible and exercisable.

Second, the Constitution further adopts a more liberal approach to the right of access to information in Article 35 by empowering Kenyan citizens with the right to information either held by the state; or information held by other persons and required for the exercise or protection of any other right or fundamental freedom. The provision goes as far as to mandate the state to publish and publicize any important information affecting the nation.[87] This provision coupled with the freedom of expression which includes the freedom to seek, receive and impart information or ideas[88] aid in public participation, a national principle of governance espoused in the constitution.[89] Moreover, the Constitution provides that the principles and values of public service include transparency, and provision to the public of timely and accurate information.[90]

Lastly, notwithstanding, Article 31 provides for the right to privacy which inter alia, includes the right not to have information relating to a person's family or private affairs unnecessarily required or revealed.

The Access to Information Act 2016

It is five years since Kenya passed a comprehensive Access to Information Act,2016. The law is rated as progressive as it guarantees access to citizens (natural and legal) and its scope is wide enough.[91] Globally, it is rated number 21 out of 129 countries whose laws were assessed scoring 113 marks out of possible 150. In Africa, the Kenyan law is rated number six only falling behind Liberia, Sierra Leone, South Sudan, Tunisia and South Africa respectively.[92] However, the necessary regulations have not been adopted hampering effective implementation. The law seeks to give effect to Article 35 of the Constitution of Kenya and confers on the Commission on Administrative Justice the oversight and enforcement functions and powers.[93]

First, the law provides for the procedures for requesting information, how to appeal against denial of information and sanctions for any violation of different Sections of the law. It does so by inter alia, providing a framework for public entities and private bodies to not only provide information upon request but also proactively disclosing information that they hold in line with the constitutional principles relating to accountability, transparency and public participation and access to information.[94]

Second, the Act contains a raft of provisions arranged into various Sections. Part II provides for the scope of the Right to information[95] which includes proactive disclosure by public entities[96] and the limitations to the right in accordance with Art 24 of the Constitution where such disclosure would undermine the national security, economy, public health or safety of Kenya, impede the due process of law, involve the unwarranted invasion of the privacy of an individual without proper authority, substantially prejudice the commercial interests of an entity or third party from whom information was obtained or infringe professional confidentiality as recognized in law or by the rules of a registered association of a profession.[97] The same Section goes ahead to list the exempt information covered under national security[98].

Third, Part III focuses on the institutional framework in place to facilitate access to information. It provides for an information officer who shall be the CEO of a public entity with the ability to delegate such powers as required to effect his/her mandate under the Act.[99] Additionally, it outlines the procedure for application of a request for access and the tentative time frame for processing such requests (within 21 days of receipt) and circumstances where extensions or transfers of applications may be warranted.[100] Responses made to such requests ought to be in writing[101] and no fees other than the costs incurred in supplying requested information are chargeable.[102] Should an information officer decline a request for information, the reasons for making that decision, including the basis for deciding that the information sought is exempt, unless the reasons themselves would be exempt information; and a statement about how the requester may appeal to the Commission must be availed.[103] The Act allows for correction of information at the public entity's cost should information supplied be inaccurate, incorrect or need updating.[104]

Fourth, Part IV concerns itself with the review of decisions of public entities by the Commission of Administrative Justice by setting out grounds for reviews, either upon application or on its own initiative.[105] More importantly, the Act protects whistleblowers, that is, persons who disclose confidential information obtained in the course of their employment provided the disclosure was made in public interest such as concerns of a breach of law.[106] The Act goes as far as to void any confidentiality agreements aimed at defeating the release of information in the public interest and even criminalizes the giving of false information with the intention of injuring another person. In an effort to facilitate accountability, the Act mandates public entities to keep accurate records,[107] and penalizes erasure, blockage, defacement or alteration of records.[108]

Fifth, Part V confers upon the commission oversight and enforcement powers that task it with reviewing decisions relating to access to information, reviewing reports on implementation of the Act. Part VI concerns regulations that are to be passed by the Cabinet Secretary in charge of Information to effect statutory provisions.[109] Part VII of the Act makes provisions for annual performance reports to the Cabinet Secretary [110], reports by public entities on information requests received and how they were handled[111] , offences and penalties[112] .

Sixth, as a result, the Commission on Administrative Justice has developed and issued a model law on access to information for county government,[113] and engaged a number of subnationals to encourage them to enact their specific access to information laws. Kilifi and Makueni are two of the studied subnationals that the CAJ has directly engaged with on this issue. [114]

Through the engagement with subnational governments, the Commissioner for Access to Information, CAJ indicated that it has seen 46 of the 47 subnational appointments and designate specific access to information officers[115]. She added that the Commission has so far received 369 applications for review and appeals on refusal to disclose information and that they have effectively resolved 332 applications (89.9 per cent). They have issued 30 enforcement orders requiring various public bodies to disclose certain sets of information to the requesters and three are pending before the High Court. The Commission has trained 7904 public officials across the country on their legal obligations under the Access to Information Act, 2016 in the last five financial years.

Seventh, internally, the Commission on Administrative Justice has given more impetus to access to information. Its second Strategic Plan (2019-2023) has access to information as a one of the four strategic areas.[116] Consequently, it has also designated an Information Commissioner and also created a standalone directorate of Access to Information.[117] However, the directorate has a very skeletal staff that may not be able to sufficiently serve all state and non-state actors on the issue of promotional education and also enforcement.

Eight, through collaboration with civil society organisations, the Commission on Administrative Justice has developed the Access to Information (General) Regulations, 2021,[118] and is in the process of engaging the Ministry of ICT and other relevant stakeholders to ensure they are gazetted and operationalised.

Lastly, citizens generally expressed their frustration when attempting to get information from their county governments public expenditure and audit reports. While all government ministries, departments, and agencies including county governments, are required as per the Executive Order number 2 of 2018[119] to post all their procurement information on the Public Procurement Information Portal (PPIP), the experience across the four counties vary. The typical information provided on the PPIP includes name of tender, amount, and the supplier, including dates. Other details on detailed descriptions or units of goods or services supplied are missing.

Judicial Interpretation on access to information

In the most high profile case concerning access to information in Kenya thus far, the jurisprudence on access to information has evolved overtime specifically influenced by the Access to Information Act. Prior to its enactment, there were alot of questions on who could lodge an access to information request under Article 35 (1) of the Constitution.

First, in ***Andrew Omtatah Okoiti V Attorney General & 2 others [2011] eKLR[120] and in Kahindi Lekalhaile & 4 others v Inspector General National Police Service & 3 others [2013] eKLR[121]*** the court laid out that the first step before approaching the court asking another party to disclose relevant information, one ought to request information directly from a concerned agency and failure to which approach the court and not the other way round.

Second, in ***Famy Care Limited vs. Public Procurement Administrative Review Board & Another & 4 others [2013] eKLR[122]*** and in ***Nairobi Law Monthly Company Limited V Kenya Electricity Generating Company & 2 Others [2013] eKLR[123]*** the court held that the right to information is only enjoyed by natural Kenyan citizens and not juristic persons such as corporations or associations. However, this position later changed in the case of ***Katiba Institute v President's Delivery Unit & 3 others [2017] eKLR*** the issues for contention, inter alia, included whether a corporate body is a "citizen" for purposes of enforcement of the right to access to information under the CoK, 2010 and the Access to Information Act; and whether Article 35 of the Constitution and Section 6 of the Act set out conditions for accessing information. The court held that Section 2 of the Act defined a citizen as any individual who had Kenyan citizenship, and any private entity that was controlled by one or more Kenyan citizens. From the definition, the Petitioner, by virtue of having Kenyan directors, though a juristic person, was a citizen for purposes of Article 35(1)(a) as read with Section 4 of the Act and was entitled to seek and have information as a citizen. In accepting the petition to compel the respondents to provide the advertisement information requested, the court further held that it was up to the Respondents to show how the information sought affected state security and therefore, fell within Section 6 of the Act. The court was not satisfied that the nature of information sought was exempt information under the umbrella of national security.[124]

Additionally, in ***Nelson O Kadison v Advocates Complaints Commission & another [2013] eKLR[125]*** the court compelled the Advocates Complaints Commission to release information as it was a statutory body and as such had obligations to respond to citizens requests for information.

Third, in ***John Harun Mwau v Linus Gitahi & 13 others [2016] eKLR[126]*** the court was called upon to determine the responsibility of the entities to comply with access to information requests where the information is necessary for the protection or exercise of another's rights. In the case, the defendants Nation Media Group had published an article accusing the applicant Mr Mwau of trading narcotics. As a consequence of the article,the US imposed travelled sanctions on the applicant. Mr Mwau made an application to court seeking to have respondents disclose information on the narcotics including location of a container and the date it was impounded by authorities. The court held that the information held by the respondents had to be disclosed to the applicant as it was necessary to enforce the petitioner's rights as per Article 35(2) of the Constitution.

Lastly, in ***Trusted Society of Human Rights Alliance & 3 others v Judicial Service Commission & another [2016] eKLR[127]*** the court balanced access to information rights and the right to privacy and compelled the Judicial Service Commission (JSC) to disclose as much as possible but respecting the right to privacy of applicants who had applied for various positions within the judiciary.

The Data Protection Act 2019

First, the Constitution of Kenya guaranteed and safeguarded the right to privacy in general and data protection in particular when it was promulgated. Data protection is one of the four aspects/facets of the right to privacy. This step ensured that the right to data protection was justiciable in Kenya. Before, citizens had to rely on the common law approach in seeking recognition and protection under the common law right to privacy.

Second, after nearly a decade of the continued lack of comprehensive legislation, on 25th November 2019 the Data Protection Act, 2019 became enforceable. The act comprehensively governs the collection, processing and storage of personal data by government and private actors.[128] It does so by establishing an intricate ecosystem of rights and obligations that operationalise the right to privacy, as espoused under the Bill of Rights.[129]

Third, in a similar fashion to the European Union General Data Protection Regulation (GDPR)[130] , the immediate focus of the Act seems to be on the processing of data.[131] In accordance with the extraterritorial nature of data, the Act applies to both resident and non-resident data processors and controllers.[132] Where the Act differs from the GDPR is in its placement of several data protection obligations on both controllers and processors, whereas the GDPR only holds data processors responsible for security and other limited requirements.

Fourth, the act rightfully documents the various principles under which data processing should be done. These include; informed consent, specificity, lawfulness, transparency, relevance and reasonable duration of storage, legitimacy, accuracy and constantly updated, non-identifiable storage of data and necessity.[133]

Fifth, the act further goes on to establish the rights of data subjects, which stem from the principle of consent. These include the right to be informed of the use to which their data is put to,[134] access their data that is in the custody of the data controller or processor,[135] object to the processing of personal data, to request the correction[136] or deleting[137] of false or misleading data and to have data that has outlived its authorised use or was collected illegally deleted[138].

Sixth, as an enforcement measure, the Act has also set various fines that are proportional to the severity of non-compliance or infringement of human rights.[139] However, the concerns related to the insufficiency of the fines proposed in the GDPR[140] are also applicable to Kenya's Data Protection Act as they simply are not high enough. Furthermore, the liberty granted through statutory exemptions create room for abuse by government agencies.[141] Finally, in a similar manner to the GDPR, the uncertainty in various Sections and the implementation of the Act may serve to defeat its purpose.[142]

However, its implementation was equally delayed for nearly a year as the process of recruiting the Data Protection Commissioner was not immediately commenced. But a month before the recruitment of the Data Protection Commissioner, the country adopted the so-called Huduma Namba Regulations in response to a series of court cases that had earlier stalled the national programme of registering all citizens and issuing them with a new biometric card or the digital identity card.[143] The Court cases were consolidated in the Nubian Rights Forum and 2 others v. Attorney General & 6 others found that Sections of the Registration Persons Act that required the collection of GPS coordinates and DNA to be in conflict with Article 31 of the Constitution of Kenya, 2010 on right to privacy.[144] The Court also suspended the use and processing of personal data collected under the National Integrated Identity Management System (NIIMS) processes until a comprehensive regulatory framework in compliance with the COK, 2010 was developed. The government has appealed the ruling at the Court of Appeal at the time of compiling this report.

A number of milestones are worth noting. First, the Office of the Data Protection Commissioner (ODPC) is now established and has a service charter spelling out details about customer rights and expected service delivery.[145] Second, the ODPC has developed three manuals and standard operating procedures. The manuals are: Manual on Lodging Data Breach Complaints; Procedure on Complaints Handling Procedure;[146] and Procedure on Carrying Out Inspection. The three offer an opportunity to data subjects, controllers and processors to engage with the ODPC and augment the law to ensure their understanding of the processes and the expected outcomes.

Third, the ODPC has worked with the Taskforce on Development of Data Protection Regulations to develop a set of implementing regulations.

The taskforce was appointed in January 2021.[147] The team has so far developed a set of proposed general and specific regulations and guidelines. Some await public participation before review by the respective Cabinet Secretary and adoption by the National Assembly. These are: the Registration of Data controllers and Processors regulation;[148] Data Protection (compliance and Enforcement) Regulations, 2021; [149] Data Protection (General) Regulations, 2021 which have a wide scope including consent of the Data subjects; collection of personal data; enabling the rights of the Data Subjects; commercial use of personal data; obligations of data controllers and data processors; data protection by design or default; notification of data breaches; transfer of personal information outside Kenya; data impact assessment and how exemptions may be applied. The Office also developed a Guidance Note on Consent. [150]

The ODPC has also initiated an engagement framework that enables her office to engage with stakeholders periodically. This has seen her partnership with Amnesty International-Kenya in conducting the first research on data governance in Kenya and also in conducting comparative research on Data Protections Commissions funding, human resources, independence and financial sustainability.[151]

The ODPC has recently also rolled out stakeholders awareness programmes for big data controllers in government through an awareness programme run jointly with Kenya School of Government.[152] The ODPC has also initiated engagement with subnational governments and raising awareness among different actors and developing contacts and networks to ensure international cooperation.[153]

The appointment of the Data Commissioner, despite the concerns related to the independence of the office, has been positively received. This is due to the crucial role that these laws will play in ensuring free and fair elections, come 2022 given the potential to counter fake news and irresponsible online political showdowns.

While these actions represent a step forward in promoting the right to privacy for the nation, there still remain a few roadblocks to the effective implementation of the Act. As noted by Privacy International, the shortcomings in the Act still need to be addressed, while the office of the Data Commissioner must, besides being made independent, be well staffed and resourced.[154]

Similarly, as employers collect and process data of their employees, they must conform to the Data Protection Act which requires the employer to explain to employees the purpose for which their data is collected and use it for a lawful purpose. Although the Act mandates the collection of data directly from employees, it also provides for certain situations where data can be collected indirectly from other sources. For example, to protect the interest of the employer or where the information is part of a public record, or collection from another source does not prejudice the interest of the employee.[155] For example, an employer who implements monitoring tools such as CCTV in the workplace may do so with consent of employees but where consent is not obtained, such processing must be for lawful purposes outlined in the Act such as protecting legitimate interest of the employer.[156] As such processing is likely to interfere with the rights and freedoms of employees. Thus it is ideal to have a policy which explains to employees: 1) the purpose of using CCTV, 2) 3rd parties with access to the footage, 3) the duration which the footage is held, 4) means by which employees can access the recorded data .[157]

Employees have a right to object to processing of their personal data where their rights override legitimate interest of employers.[158] The draft Data Protection (General) Regulations provides the procedure employees can use to object to processing and employers have 14 days to comply with such requests.[159]

Lastly, in a similar fashion, the government at both national and subnational level collects and processes personal data of citizens. The Information collected by the government in a digital format is often what is prescribed in manual forms as per legislation. Regardless, the government has a responsibility to comply with the data protection act and implement technical and security safeguards to protect data collected.An example is the Land Registration (Electronic Transaction) Registration 2020 that creates the National Land Information Management System for the electronic transfer of land, provides for terms and conditions to use the system. The conditions contain a data privacy statement that explains the nature of personal data collected, purpose, third parties who may be granted access to the data, technical and security measures to safeguard data and the right of data subjects[160] . As Kenya adopts e-governance and more public services are available over digital platforms like e-citizen, there is a need to harmonise laws and ensure they conform to the data protection Act.

Judicial Interpretation on data protection

In the most high profile case concerning data protection in Kenya thus far, the high court ruled that the laws on data protection that were presently available were insufficient.[161] Therefore prior to the Data Protection Act, the court ruled on the issue based on the Kenyan Constitution and the global principles related to Privacy. These principles mostly emanated from Kenya's participation in the international community.

The courts often relied on the principles discussed in the Background section of this paper found in 4 critical instruments at the international level that obligate states to guarantee data protection and privacy rights to citizens and 11 critical instruments at the international level that provide principles that states should consider in order to facilitate data protection and the right to privacy rights of Kenyan citizens. All these principles are applied globally and implement Article 12 of the Universal Declaration of Human Rights (UDHR). These are found in: Universal Declaration of Human Rights (UDHR)[162] , International Covenant on Civil and Political Rights(ICCPR)[163] , African Charter on Human and People's Rights (ACHPR),[164] the African Union Convention on Cyber Security and Personal Data Protection,[165] African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa,[166] the United Nations Guiding Principles on Business and Human Rights,[167] the Tunis Agenda for the Information Society (World Summit on the Information Society-WSIS), [168] the Seoul Declaration for the Future of the Internet Economy (OECD),[169]the Ten (10) Internet Rights and Principles (Internet Rights and Principles Dynamic Coalition), [170] the NETmundial Multistakeholder Statement (Conference Outcome),[171] the UN Human Rights Council (HRC) resolution on "the right to privacy in the digital age", [172] the Resolution 362 of The African Commission on Human and Peoples' Rights (ACHPR),[173] the African Declaration on Internet Rights and Freedoms,[174] the International Principles on the Applications of Human Rights to Communications Surveillance (Necessary and Proportionate Principles),[175] and the Global Principles on Freedom of Expression and Privacy.[176]

These international instruments have been critical to interpretation of the right to privacy in Kenya even before enactment of the Data Protection Act 2019.

Some of the notable Kenyan cases interpreting the principles include the following:

Firstly, in ***Okiya Omtatah Okoiti & 2 others v Attorney General & 3 others [2014] eKLR,*** the petition could not stand because the evidence upon which it was premised was privileged communication between the State and Exim Bank of China and which should not have been fraudulently obtained especially given that there are lawful means of obtaining such information including compelling the state through the right to information. The privacy of the respondents was therefore held to have been infringed and the petition dismissed[177] .

In this judgement, the court affirmed the principle of legality by stating that there already existed lawful means to obtain the evidence premised upon in the petition and further relied on the Principle of Safeguards against illegitimate access and right to effective remedy[178] which states;

"States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected."

Second, in ***Samson Mumo Mutinda v IG National Police Service & 4 others [2014] eKLR*** it was established that the petitioner's right to privacy had not been infringed after his driving school registers and mobile phones were seized without a warrant by police during investigations because a search had been done with the petitioner's consent. The court found that he had failed to object the search even after understanding the nature of the investigation underway[179].[3]

In this judgment, we can note that the court relied on the principle of User notification or the principle of consent and legitimacy of personal data processing and drew attention to the fact that once one consents to a search without a warrant including during investigations and media interviews can be consented away respectively, they would not be able to pursue recourse for breach of privacy thereafter.

Third, in ***Bernard Murage v Fineserve & 3 others [2015] eKLR***[180] it was found that in cases where consumers have consented away certain data protection and privacy rights in regard to the terms and conditions attendant to the use of certain technology being sold to them by a telecommunications provider, then the operator cannot be held liable for violation of the right to privacy and consumer rights even in the absence of a comprehensive data protection law.

It was held that the Thin SIM technology is relatively safe in banking and any risks would be dealt with by the relevant bodies[181] .

We can note that the court affirmed the principle of legality, necessity and proportionality. In addressing the principle of legality, the court provided under paragraph 56- 58 and 62-64 of the judgement, whereby the court affirmed for protection of the right of privacy when it has been threatened to be infringed but not necessarily requiring proof that the right has been infringed. The court also referred to the principle of legality when it reaffirmed that there must be precision in the law for one to seek a remedy for violation of their rights.

Fourth, in ***JWI & another v Standard [2015] eKLR*** The Standard and Nation Media Groups were found not to have infringed privacy rights of the children of a wanted man after they published articles including pictures of the man. It was held that while the privacy of the minors had indeed been infringed, these rights had been waived by their mother, who consented to their pictures being taken at the time of interviewing the family[182] .

In this judgment, we can note that the court relied on the principle of User notification or the principle of consent and legitimacy of personal data processing as it applied to minors and emphasized that parents and guardians are the custodians of the right to privacy of their children.

Fifth, in ***Roshanara Ebrahim v Ashleys Kenya Limited & 3 others [2016] eKLR,*** Ms Ebrahim who had been crowned Miss World Kenya 2015 petitioned the court as a result of her being dethroned based on leaking of nude photographs of her to the Miss World Kenya organisers by her boyfriend. The court determined that the Bill of Rights applied equally to a private citizen as an obligation of both state and non-state actors in terms of Article 20 of the Constitution. The court emphasized that,

"..The 3rd Respondent had by his close relationship as a boy-friend of the petitioner accessed the petitioner's photographs, and may indeed have taken some of them, but he had no authority to publish the private photographs. In forwarding the private photographs of the petitioner to the 2nd respondent, the 3rd petitioner had violated the petitioner's right to privacy of information under Article 31 (c) of the Constitution, and the petitioner is entitled to compensation in damages..."

In this judgement, the court addressed the principle of legality, and affirmed Article 31 (c) of the Constitution provides for the right to informational privacy which includes privacy of private photographs of a person. Additionally, the court was guided by the principle of User notification or the principle of consent and legitimacy of personal data processing, and the Principle of Safeguards against illegitimate access and right to effective remedy. The court demonstrated that an individual had a reasonable expectation of privacy extending to lawful communication between two people in a relationship. Whereas Ebrahim might have consented to possession of the nude pictures by her boyfriend, she had not consented to any sharing of the same to third parties.

Sixth, In ***N W R & another v Green Sports Africa Ltd & 4 others [2017] eKLR,*** the court reaffirmed that parental consent is mandatory as it regards limiting the right of minors privacy and determined the scope under which parental consent is granted. The court required documents to be signed by the minor's parents or the respondent to provide evidence that this was brought to their attention. Additionally, the court reaffirmed liability of privacy violations as it regards minors to include a respondent: (i) Use of a Protected Attribute, (ii) For an Exploitative Purpose and (iii) without consent.

In this judgment, we can note that the court relied on the principle of legality, principle of User notification or the principle of consent and legitimacy of personal data processing as it applied to minors and emphasized that parents and guardians are the custodians of the right to privacy of their children.

Seventh, in ***Gloria Jepkurui Koima Vs KPMG Advisory Services (Cause.2612/2016)***[183] the court determined that the audit firm, KPMG had violated Ms Gloria Jepkurui Koima's rights to privacy, as a result of seizure of her personal phone without her consent and use of personal information obtained in disciplinary proceedings in the firm.

In this case, the court was guided by the principle of User notification or the principle of consent and legitimacy of personal data processing, and the Principle of Safeguards against illegitimate access and right to effective remedy. The court demonstrated that employees had reasonable expectations for privacy of data held in their personal devices. The court emphasized that information ought to be obtained in a lawful manner under conditions where the person is well informed and grants unequivocal consent of the use of personal data.

Thus from the limited jurisprudence available, it is clear that the operation of the Data Protection Act is yet to fully take effect, on account of the challenges it has faced under law and its relative recency.

Consumer Protection Act, 2012

First, the Act was enacted to give effect to the right to consumer protection provided for under Article 46 of the Constitution by improving consumer awareness and encouraging responsible and informed consumer choice and behaviour. Part I of the Act[184] states the objects and purpose of the Act which is to protect consumers from all forms of unconscionable, unfair, unreasonable, unjust, or otherwise improper trade practices and reduce any disadvantages experienced by consumers in accessing supply of goods and services.

Second, it is important to note that the Act broadens the definition of a consumer beyond just the user of goods or services to include; '*a person to whom goods or services are marketed in the ordinary sense of a suppliers business.*[185] '

The growth of the digital economy has led to an equal growth in digital marketing. Conversely, there is a responsibility for advertisers to be prudent in supplying adequate and relevant information to ensure a consumer is able to make informed choices on digital products, especially where face to face interaction is completely eliminated in the supply chain.

Section 31-33 specifically deals with the regulation of internet agreements, an agreement formed by text based internet communications. The act requires a supplier of goods or services to provide the consumer with all relevant material information in a format which the consumer can retain and print and an express opportunity to accept, decline or correct the agreement before entering into it. Failure to do this gives the consumer a right to cancel the agreement.

Third, Part II of the Act elaborately provides for consumer rights including the prohibition of advertising an illegal gaming site, operated contrary to the law. The researchers note that this part complements the 2021 Draft Data Protection (Registration of Data Processors and Controllers) Regulations which will also require gaming sites to register as data protection controllers and processors.

Fourth, Part VII of the Act deals with credit agreements, an agreement in which the lender extends credit or lends money to a borrower but does not include an agreement where a borrower obtains credit on security of mortgage of real property. The Act requires lenders to issue borrowers with a disclosure statement prior to entering into a credit agreement. The Act also protects consumers by prohibiting advance payment for credit repairs until the credit repairer causes improvement to a the credit information, rating or history of consumer[186].

Fifth, in a report released in September 2021, 55 out of 100 participants surveyed had acquired loans from digital lenders.[187] To date Kenya has at least 49 digital credit providers whose credit services are attractive because they are convenient, easy to access and have fast loan remittance[188] . However,some of these digital lenders engage in aggressive debt collection that includes debt shaming and misuse of personal data.[189]

Sixth, in order to ensure consumer protection and data protection with regards to digital lending, Kenya is seeking to enact the Central Bank of Kenya (Amendment) Bill 2021 which complements the Consumer Protection Act, 2012. The National Assembly Departmental Committee on Finance received public comments on the bill and recommended the need for sector regulators specifically the Central Bank, office of the Data Protection Commissioner and the Communications Authority to work together to ensure data and consumer protection in the digital lending Sector[190]. The committee also introduced amendments to the CBK (Amendment) Bill that regulate debt shaming.[191]

Lastly, Part X of the Act also establishes the Kenya Consumers Protection Advisory Committee to monitor enforcement of the law, develop relevant policies and conduct consumer awareness on consumer protection.

The Kenya Information And Communication Act, 1998- Revised Edition 2011 (2010)

Additionally, the Act establishes the Communications Authority of Kenya as an independent body to license and regulate postal, information and communication services[192] while respecting freedom of the Media[193] . As limitation of media rights must comply with the Constitution, this promotes the free flow of information. The Authority has a responsibility to ensure telecommunication services are provided throughout Kenya, regulating the pricing of services, ensuring quality of service and processing of personal data is done in accordance with the Data Protection Act 2019[194]. Additionally, the Act creates the Universal Service Fund (USF) that is used by the Authority to promote access to ICT services especially in unserved and underserved areas in Kenya.[195] To date the Authority has used the USF to fund projects like; the Education Broadband Connectivity Project that increases broadband connectivity in schools[196].

Second, the Authority has also set up the National Kenya Computer Incident Response Team to undertake technical coordination of cyber incidents and promote awareness on cybersecurity.[197] This ensures Kenya is able to respond to cyber incidents that threaten the access to information, privacy and data protection rights of its residents.

Third, in a bid to increase broadband connectivity in unserved and underserved areas in Kenya, promoting access to the internet and converse access to information, the Authority is considering a licensing framework for community networks in Kenya. In May 2021, the Authority published the draft Licensing and Shared spectrum framework for Community Neworks[198].

Fourth, the Act prohibits licensed telecommunication operators from intercepting, outside the ordinary course of business, a message sent through a licensed telecommunication system or disclosing any information from the interception to another person[199] . This ensures confidentiality of communication for consumers. In addition, the Act allows the authority to either comply with access to information requests or restrict access to information in conformity with Article 35 of the Constitution[200] .

Lastly, the Act gives the Court powers to grant the commission a search warrant to enter and seize any article or thing necessary to prove an offence under the information and Communication Act is being or has been committed, this may include recovery of data[201] .

The Kenya Information and Communication (Consumer Protection) Regulations 2010

First, these regulations provide for rights and obligations of customers of any licensed operator under the Act. The customer has a right to information about the terms and conditions of any service and personal privacy and protection from unauthorized use of a subscriber's personal information[202] .

Lastly, the regulations also require that licensees establish mechanisms to enable parents or guardians to block access of children to harmful content. It also makes it an offence for licensees to promote marketing of harmful substances including alcohol or tobacco to children[203]. Additionally, as part of the Authority's responsibility in protecting children, the Authority runs the Child Online Protection campaign named 'Be a COP' that promotes awareness on child online protection to parents and guardians. It has also created a portal to receive and investigate incidents involving minors online.[204]

Finance Acts:- Finance Act of 2019, Finance Act of 2020 and Finance Act of 2021

Over the last decade, Kenya has introduced digital taxes through various legislations such as the Finance Act of 2019,[205] Finance Act of 2020[206] and Finance Act of 2021[207] which all impact the cost of internet affordability or affordability of digital supplies, raising the cost of accessing information.

First, the Finance Act of 2019 amended Section 3 of the Income Tax Act to include the definition of the digital marketplace currently defined as; an online or electronic platform that enables users to sell or provide services, goods or other property to other users.

Second, in 2020, the Finance Act introduced the Digital Service Tax, a tax levied on income derived from a digital marketplace. The Tax is levied on taxable supplies such as subscription based media including news, magazines and journals, or over the top services including streaming tv shows, films, podcasts etc. Following the introduction of DST, pricing in several services such as Netflix Plans for Kenyan consumers increased[208]. This, as stated, increases the cost of accessing information.

Third, the 2021 Finance Act introduced further additional changes to the Digital service Tax to provide more clarity on its applicability[209] .

Lastly, the 2021 Finance Act also increased the rate of excise duty in Kenya from 15% to 20%. This increased the cost of voice calls, data and SMS offered by telecommunication operators in the country, again raising cost of communication and access to information[210].

National Intelligence Service Act, 2012

First, it is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The Act was primarily enacted to provide for the functions, organization and administration of the National Intelligence Service (NIS) pursuant to Article 239(6) of the Constitution concerning national security organs; to give effect to Article 242(2) on establishment of the NIS and to provide for the establishment of oversight bodies.[211]

Second, Section 42 of the Act provides for ex-parte application of warrants to the High Court in order to enable the Service to investigate any national security threats or perform any of its functions.[212]

Limitations on the right to privacy espoused in Article 31 of the Constitution may be limited in respect of a person suspected to have committed an offence to the extent that subject to Section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with, having obtained the proper warrants.[213]

Third, in April 2020, the Court of Appeal reversed a High Court decision precluding the government's plan to implement the Device Management System (DMS), a mechanism for identifying counterfeit and illegal phones. [214] The High Court had ruled that the system, which gives the CA access to mobile subscriber data, including call records, would infringe on subscribers' right to privacy, among other concerns.[215] The Court of Appeal ruled that the High Court lacked evidence to reach this conclusion.[216] In June 2020, after the coverage period, the Law Society of Kenya appealed the case to the Supreme Court; though the DMS will be implemented while the appeal is being considered.

The National Computer and Cybercrimes Coordination Committee, whose membership includes the NIS has also been established to advise and coordinate national security organs on matters relating to computer and cybercrimes.[217]

Fourth, in the case of ***Coalition for Reforms and Democracy (CORD) & 2 others v Republic of Kenya & 10 others,*** the court observed that the monitoring of communication and searches authorised by Section 42 of the NIS Act, (as amended by the National Security Laws Amendment Act, 2014) contains safeguards in the exercise of the powers under the Section. The new Section requires that the information to be obtained under Section 42(3)(c) must be specific, shall be accompanied by a warrant from the High Court, and will be valid for a period of six months unless extended.[218] Consequently, the court held that this contested provision, albeit limiting the right to privacy, is justifiable in a free and democratic state,[219] and therefore not contrary to the right of privacy guaranteed in Article 31 of the Constitution.[220]

Lastly, the right to privacy and the right of access to information set out in Article 35 (1) and (3) of the Constitution may be limited in respect of classified information, information disclosing or publicizing information relating to sources of information, intelligence collection methods or covert operations, or information that would otherwise undermine national security.[221]

Prevention of Terrorism Act, 2012

First, it is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The Act was enacted with the primary purpose of providing for measures for the detection and prevention of terrorist activities.[222]

Second, the Act confers police officers with powers to make ex-parte applications to a Magistrate's Court to gather information when investigating suspected terrorist activities.[223] The Act further provides for limitation of certain rights subject to Article 24 of the Constitution in the pursuance of terrorism investigation, detection or prevention.[224] Limitation to the right of privacy extends to allowing a person, home or property to be searched; possessions to be seized or the privacy of a person's communication to be investigated, intercepted or otherwise interfered with.[225] Limitations on the rights of accused persons under Article 49 of the CoK, 2010 can also be limited to the extent that is necessary for the protection of the suspect or any witness.[226] The freedom of expression, the media and of conscience, religion, belief and opinion may also be limited to the extent of preventing the commission of an offence under the Act.[227]

Third, the Act further empowers a police officer of or above the rank of Chief Inspector of Police to make an ex-parte application to a Chief Magistrate or to the High Court for an interception of communications order.[228] In the same breadth, national security organs are also empowered to intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary.[229]

The Act goes as far as to impose a sanction-backed positive obligation on all persons to disclose any information pertaining to terrorist activities.[230]

Fourth, the court in the case of ***CORD & 2 others v Republic of Kenya & 10 others,*** held that the prohibition on the publication or broadcast of images of dead or injured people, which are "likely to cause fear and alarm in the general public, or disturb the peace", was disproportionate. The Court found that there was no rational connection between the limitation on publication and the fight against terrorism thereby declaring Section 12 of the Security Laws (Amendment) Act and Section 66A of the Penal Code unconstitutional for violating the freedom of expression and the media guaranteed under Articles 33 and 34 of the Constitution.[231]

Additionally, Section 64 of Security Laws (Amendment) Act which introduced Sections 30A and 30F to the Prevention of Terrorism Act was unconstitutional for violating the freedom of expression and the media guaranteed under the Constitution. The amendments sought to criminalize publication of "offending material" that is likely to either directly or indirectly incite terrorism activities[232] or the broadcast of information which undermines investigations or security operations by the national police and defense forces.[233] The Court held that the effect of the prohibition would amount to "a blanket ban on publication of any security-related information without consulting the National Police Service.

Lastly, a Committee was established to formulate and supervise the implementation of UN resolutions relating to the suppression of terrorism financing as well as the National Strategy and Action Plan on Counter Financing of Terrorism.[234] It is empowered to coordinate with the relevant competent party, person or foreign country for the purposes of discharging its mandate.[235]

Mutual Legal Assistance Act, 2011

First, the Act was enacted with the primary aim of providing for mutual legal assistance to be given and received by Kenya in investigations, prosecutions and judicial proceedings in relation to criminal matters.[236] It is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The Act establishes the office of a Central Authority to perform functions specified under the Act and mandates the Attorney General to hold such office.[237]

Second, Part IV of the Act provides for the interception of communications, preservation of communications data and covert electronic surveillance. Kenya may, for the purpose of a criminal investigation execute a request from a requesting state for the interception, recording and transmission of telecommunications;[238] preservation of communications;[239] or for the deployment of covert electronic surveillance.[240] These requests shall be made in the prescribed manner and shall be executed in accordance with the Act and any other applicable Kenyan laws.[241] Finally, the confidentiality of a request, its contents and the information and materials supplied under the Act shall be upheld except for disclosure in the criminal matter specified in the request and where otherwise authorized by the other state.[242]

Lastly, the government launched guidelines for Mutual Legal Assistance and International Co-operation in an effort to curb cross-border organised crime by strengthening the existing cooperation which Kenya has with its diverse partners. The guidelines provide a framework that will greatly assist authorities in investigations, consultations, prosecutions, judicial proceedings, service of overseas processes and instances where the Government intends to freeze or confiscate property acquired from proceeds of crime.[243]

The Computer Misuse and Cybercrimes Act, 2018

First, it is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The Computer Misuse and Cybercrimes Act came into force in 2018. The intentions behind the enactment of the law were to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes.[244]

Second, the operation of this law is crucial to the implementation of data protection and access to information, due to the growing commercial value of data, which incentivises cybercrime geared towards data leaks and the invasion of privacy at a large scale.[245]

However, thus far the utilisation of the Cybercrimes Act has tilted towards limiting the constitutional right to access to information.[246] This is despite the fact that a very specific focus has been placed on the said right, along with the protection of the right to privacy and freedom of expression.[247] In The Bloggers Association of

Kenya v Attorney General & 3 Others, the implementation of the Act was challenged, based on its potential to infringe on the privacy of individuals, freedom of expression, speech, opinion and access to information online.[248] The high court responded by suspending certain Sections of the Act based on the principle of unconstitutionality.On full determination of the case in February 2020, the court upheld the constitutionality of the entire Act and this matter is now subject of appeal.

Third, thus far, the precedent set based on the Cybercrimes Act has been limited, as majority of the cases making references to the law have involved challenges to its constitutionality, prosecutions based on illegally obtained data that would undermine the freedom of access to information [249] and decisions that have labelled the provisions relating to data protection insufficient.[250]

Fourth, with regards to data and its related offences, the Act lists the fraudulent use of electronic data under Section 38.[251] It further goes on to provide for the procedures to be followed when seizing, accessing and processing evidentiary material from electronic data.[252] Lastly, the Act also makes provisions for the procedures to be followed following cross-border and international transfers and processing of data.[253]

Lastly, in making the above provisions, the Cybercrimes Act borrows heavily from the principles of Data Protection contained under Part IV of the Data Protection Act.[254] The enforcement of these provisions to the processing of data remains largely unexplored due to the inefficiency of cybercrime detection infrastructure in Kenya and the human rights based impediments related to the implementation of the Act.

Kenya Standards Act, 2012

First, it is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The Act was established with the aim of providing measures for the standardisation of commodities, their specification and the codes of practice.[255] The Act further establishes the National Standards Council whose functions include to supervise and control the management of the bureau.[256] The council is given the power to declare a specification or code of practice as a Kenyan standard. Furthermore, they can make amendments, replacements or abolish existing standards. However, they are required to do so by way of issuance of gazette notices.[257] Moreover, it is required that the minister establishes through a gazette notice a period after which no person shall manufacture or sell any commodity unless it complies with the code of practice.[258]

Second, recently, KEBS approved 40 new standards to enhance information and cybersecurity and safeguard consumer privacy. The standards outline techniques and methods of securing corporate information through managers charged with the responsibility of data safety. Moreover, they stipulate a framework to ensure privacy of ICT systems storing and processing personally identifiable information.[259]

Third, KEBS also adopted an Access to Information Policy in line with the Access to information Act in 2019. It outlines the responsibility of KEBS in regard to access to information to the public. It provides for the expeditious disclosure of information to any person at a fee. Furthermore, highlights the information that can be disclosed, limitations and establishes the information Access Officer.[260]

Fourth, the Minister is required at the end of every financial year to publish a report of the Agency's financial position to parliament in relation to the fund created under Section 8 of the Act. [261] This access to information enables the legislature to act as a watchdog for the agency in an effort to ensure accountability and transparency in the agency.After, the report should be made available to the public.

Lastly, the implementation of this Section has begun with the financial statements for the year 2017 and 2018 being published on the KEBS website for public access. However, no further updates have been made since then.

County Government Act, 2012

First, it is important to highlight this Act as the institutions established by the Act are important for both national and county governments. The County Government Act was established in 2012 with the aim of giving effect to Chapter eleven of the Constitution. This entailed providing for the powers, functions and responsibilities of the county government. [262]

Lastly, Access to information in the Act is provided for under Part X. It provides for the right of every citizen upon request, to have access to information held by any county government or any other state organ.[263] It goes further to make provisions for every county government to designate an office to be used to ensure access to information. [264] Moreover, it obligates the county government to enact legislation to ensure access to information subject to national legislation. [265] The county is also required to facilitate access to information through media with the largest public outreach.[266] The right to access information is seen as a window in enforcing other rights such as that of public participation. For the public to be able to effectively take part in the affairs of their community and the country as a whole, they need to have access to accurate information.[267] The Act recognizes that timely access to information as one of the main principles influencing citizen participation in the management of a county government.[268] The county government is mandated to allow public sittings during the law formation process to allow citizens to take a proactive role in the formation of these laws and projects. [269]

Subnational Level

First, each of the 47 subnationals in Kenya have rolled out different measures, procedures and in some cases regulations and policies to fulfil their obligations to protect, promote and fulfil both the right to access information and the right to privacy for its citizens in general and to ensure personal data protection in particular.

Second, county governments collect data on citizens on a number of occasions. These include public events, when citizens are applying for various permits from the county government, and for purposes of enabling the county governments to offer an array of services. The study investigated whether citizens are aware that their personal details are being collected by county governments, and how they perceive the data usage. In both the structured questionnaire survey and focus group discussion sessions, citizens expressed awareness that county governments collected their personal data.

Third, with regard to the safety of personal data of citizens, we sought to establish county government officials' perceptions of the safety of citizen data. The table below presents the findings on this aspect. The data on Makueni was not obtained by the time of writing this report.

Table 5: How would you rate the County Government's capacity to protect citizen data?

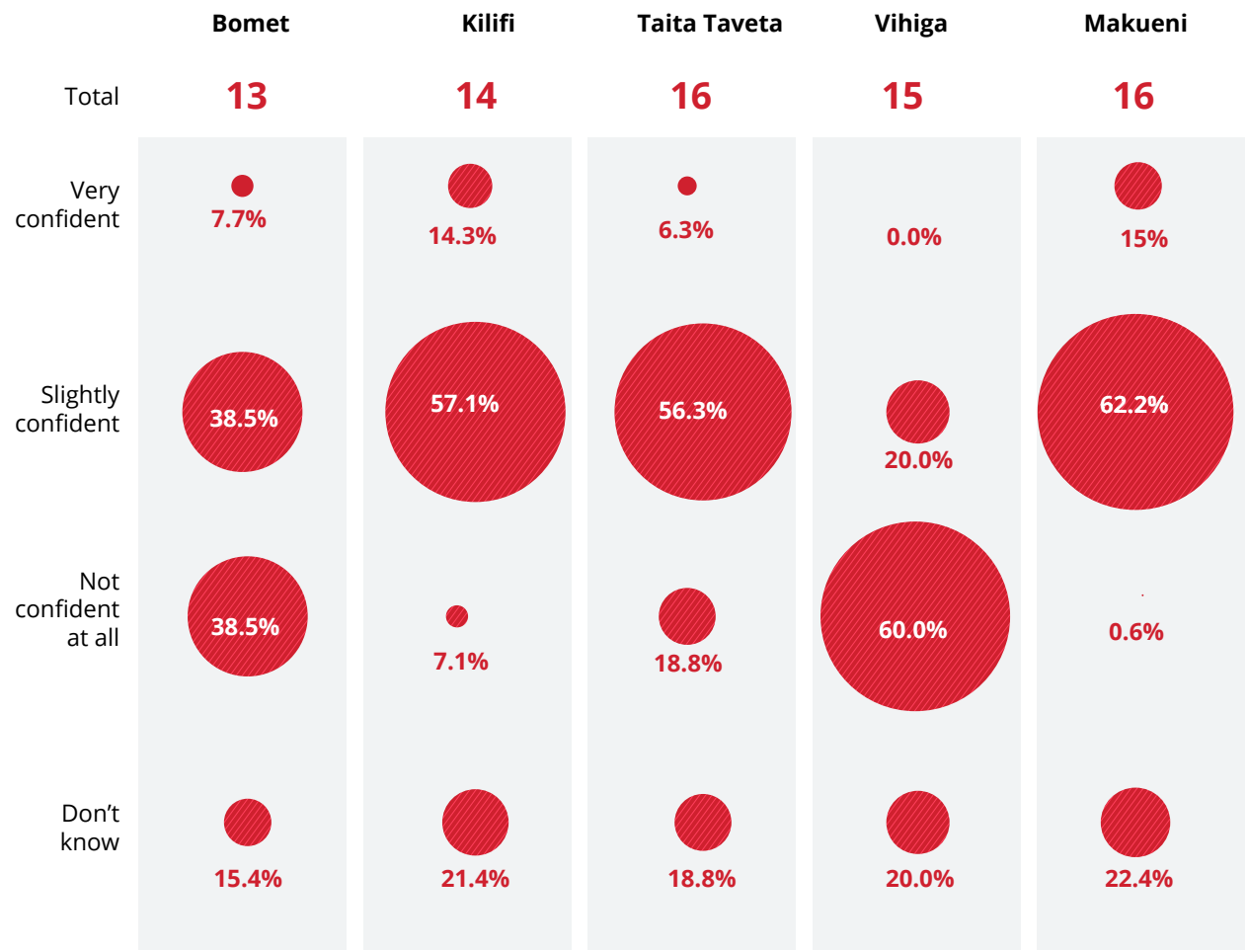
	Total	Bomet	Kilifi	Taita Taveta	Vihiga
Total	58	13	14	16	15
A. Very High	17.2%	23.1%	0.0%	18.8%	26.7%
B. Moderate	50.0%	53.8%	42.9%	43.8%	60.0%
C. Very Low	31.0%	15.4%	57.1%	37.5%	13.3%
D. Don't know	1.7%	7.7%	0.0%	0.0%	0.0%

Fourth, though county government officials were very confident (50 percent) that the citizen data in their custody is secure, a significant number of public officials lacked information on data protection and access to data laws, policies and procedures within their respective subnationals. This is because there are no dedicated personnel dealing with the data protection docket except those working in the human resources. Similarly, when asked about how likely they thought citizen data could be put to unauthorized use, 14.3 percent of the officials thought this was highly likely, 42.9 percent thought it was possible but not very likely, while 38.1 percent reasoned that it was highly unlikely. Combined, the percentages of those holding the, highly likely and possible but not very likely views, give 57.2 percent which is a clear indicator that data subjects are likely to suffer data breaches in the status quo.

Fifth, the views of county government officials differed from those held by ordinary citizens. For instance, only 6.9 percent of all citizens interviewed across four counties – Makueni excluded - are confident that their personal data which includes details on birth, death, travel, passports, marriage, elections, tax, drivers, education, health insurance and social security and education details, held by either national or county governments cannot be put to unauthorized use; 21.4 percent are not confident at all, while 50 percent mentioned that they are slightly confident.

Lastly, the table below presents citizen perceptions of data protection and privacy. Counties collect personal data in hospitals and health centres. These include sensitive personal data on medical records. It collects personal data on land ownership etc

Table 6: Citizen perception on safety of personal data collected by the County Government from abuse, or unauthorized use



Below we discuss the situation and emerging realities in the five counties in the study.

Taita Taveta County

First, the study reached 16 citizens and four county officials-two each from the county assembly and the county executive- purposefully sampled.

Second, the county government and the county assembly officials' level of awareness on the Access to Information Act, 2016 and their obligations is relatively average. This is because 50 percent seemed to know their obligations and the centrality of access to information in building trust in county government and the services they offer.[270] In fulfilment of Section 7 of the Access to Information Act, the county has designated information officers. During the study, the public officials indicated that there were information guidelines shared with information officers to follow strictly. However, we were not able to receive the guidelines when we requested for them.

Third, the researchers note that Taita Taveta has the ***Taita Taveta County Health Services Bill, 2020***[271] . Under Section 25 of the Bill, the Bill explicitly provides for Confidentiality of information on all users with information being disclosed under patient's consent or under order of court or for health research and policy planning purposes. The researchers note that this document is still a Bill and not yet an Act and thus has not been fully operationalised.

Fourth, Taita Taveta reported widespread use of Facebook, WhatsApp and other social media platforms. WhatsApp groups formed and managed by citizens themselves are much freer, and people can express their feelings freely. These platforms are typically used by younger people. However, in WhatsApp groups that are established by public officials in county government and used largely for information dissemination but rarely as platforms for debate or accountability.[272] This is because the rights to post a comment are limited to a few administrators. Respondents in Taita Taveta mentioned intimidation of people who held divergent opinions, or in extreme cases, removal from WhatsApp groups. In such cases, citizens opt to form their own.

Fifth, one of the officers pointed out that the use of websites to disseminate official information has not worked well for the locals as the region does not have reliable internet and use of mobile data remains quite expensive for the bigger population.[273]

Sixth, The study finds that two clear challenges persist. On one hand, the county continues to fail to meet its obligations Section 17 (c) of the Access to Information Act that requires it to have "computerised and digitised its records and information management systems in order to facilitate efficient access to information." [274] Secondly, the county government and county assembly have not for the last five years submitted annual reports to the CAJ as required by law.[275] On the other hand, the level of awareness about the data protection law among the county government and county assembly officials is high. All the officers interviewed except one did not know of the existence of the Data Protection Act, 2019. However, there is a low understanding on what are the legal obligations and the minimum data protection principles that must inform each and every department of the county government and county assembly. The county assembly and County service Board did not see themselves as having any clear obligations.

Seventh, there seemed to be a consensus that the revenue department had the highest obligation in safeguarding personal data obtained while offering services to the citizens. This findings clearly shows that there is need to create sufficient awareness among the public officials at the county to understand that nearly all departments and sectors collect or process personal data and yet none of them have conducted any Data Protection Impact Assessment to understand attendant risks and how best to mitigate.

Lastly, one novel action in the county was observed. The County Gender working Group is developing a tool to help collect and aggregate data on sexual and gender-based violence in the county.[276] This is because there are anecdotal cases reported and yet the National Council of Population and Development data shows that last year alone more than 1000 cases of defilement that led to pregnancies among under-age girls. The group brings together actors from the police, courts, children officers, educational institutions, CSOs and hospitals. Once finalised, the tool will be presented to the county assembly for adoption.

This approach shows there is a big opportunity to use data to develop policies and intervention strategies to handle and address a social issue in the county. However, there was no indication that in the development and deployment of the tool sufficient consideration was made on how to best centralised storage and archival of such a database shall ensure that sensitive personal data is duly safeguarded and protected.

Kilifi County

First, the study respondents were 14 citizens and four county officials-two each from the county assembly and the county executive- purposefully sampled.

Second, 100 percent of the Kilifi county government and county assembly officials interviewed[277] mentioned that their county has policies and procedures on public access to information.

Third, the citizens and county government officials' level of awareness on the Access to Information Act, 2016 and their obligations is high. This is because they formally engaged with the Commission on Administrative Justice. The county has designated information officers. During the study, the public officials indicated that there were information guidelines shared with information officers to follow strictly. However, we were not able to receive the guidelines when we requested for them.

Third, the researchers note that Kilifi has the ***Kilifi County Maternal, Newborn and Child Health Act, 2016***[278] . Under Section 25 of the Act, it explicitly provides for Confidentiality of information on the HIV/AIDS status of children with information being disclosed under patient's consent or under order of court or for the purpose of legal proceedings. The researchers note that this document only focuses on children and does not focus on all citizens.

Fourth, of the citizens engaged in the study, 40 percent were able to access information on request. The information received was largely related to health records and rates payable for land and business permits.

Fifth, the Kilifi electronic Development Administration and Management System (eDAMS) is one unique project in the coastal county. The project is made possible through partnership with the World Bank Group/ International Finance Corporation (WBG/IFC). It targets the property developers in the County and aims at enhancing access to Development Planning Certificates and Construction Permits and includes a Business Intelligence module designed to generate timely and quality reports for use by the management in decision making. Under Development Planning, the County has automated the following services: Subdivision of land; change of user; consolidation; change of user and consolidation; consolidation and subdivision; and extension of user.

Sixth, under Construction Permits the County has automated the following services: Construction Permit; Building Inspection; and Occupation Certificate.

Lastly, there was no indication that the development and deployment of the system was informed by a clear and comprehensive data protection impact assessment and does not tell us who will have access to the data.

Bomet County

First, the study respondents were 13 citizens and eight county officials-two each from the county assembly and the county executive- purposefully sampled.

Second, the county government and the county assembly officials' level of awareness on the Access to Information Act,2016 and their obligations is high at a score of 85.7 percent. The county continues to fail to meet its obligations Section 17 (c) of the Access to Information Act that requires it to have "computerised and digitised its records and information management systems in order to facilitate efficient access to information."[279] Secondly, the county government and county assembly have not for the last five years submitted to the Commission on Administrative Justice annual reports as required by law.[280]

Lastly, the level of awareness about the data protection law among the county government and county assembly officials is high. The County secretary[281] seemed very informed on data protection but indicated that while access to databases is restricted to all others but seemed to allow unfettered access to ICT officers.

Makueni County

First, the study respondents were 13 citizens and eight county officials-two each from the county assembly and the county executive- purposefully sampled.

Second, in Makueni, involvement at the lowest two levels, the village People's Forum,[282] and the Village Clusters People's Forum, was seen as fairly participatory. The public participation structure has six levels namely: Village People's Forum; Village Clusters People's Forum; Sub-ward People's Forum; Ward People's Forum; Sub-County People's Forum; and County People's Forum. In order to facilitate civic education from the lowest level, three ward representatives from each of the thirty wards are identified and trained as trainers of trainers (TOT). They are also referred to as Public Participation Facilitators. Beyond this level, respondents maintained that county government consultations processes with citizens continue to reach only a few of them.

Third, the public officials level of awareness on the Access to Information Act,2016 and their obligations is high. They all seemed to know their obligations and the centrality of access to information in building trust in county government and the services they offer.[283] In fulfilment of Section 7 of the Access to Information Act, the county has designated information officers. During the study, public officials from Makueni County indicated that there were information guidelines shared with information officers to follow strictly. Makueni showed a big difference as it has in place a *county disclosure and Communication policy*.[284] The policy sets a broad framework for disclosure of county government information to third parties through various communication platforms and channels.

The policy states that the County Government is obligated to provide the public with timely, accurate, clear, objective and complete information about its policies, programmes, services and initiatives. It adds that the County Government is committed to providing timely, consistent and fair disclosure of public information held by it to enable informed and orderly market decisions by investors and other interested parties.

The researchers acknowledge the policy is well implemented allowing proactive disclosure of information. The county has information outreach sessions through its quarterly newsletter ENE: The Makueni People's Magazine. The newsletter provides information on what the county has implemented in various sectors. It also provides a platform for commentary and reviews of the county performance from citizens through letters to the editor. The county also often runs radio programmes on Musyi and Mbaitu FM especially on their agricultural initiatives.

Fourth, the researchers note that Makueni has the ***Makueni County Maternal, Newborn and Child Health Bill, 2017***[285] . Under Section 24 of the Bill, the Bill explicitly provides for Confidentiality of information on HIV status of children with information being disclosed under patient's consent or under order of court or for the purpose of legal proceedings. The researchers note that this document is still a Bill and not yet an Act and thus has not been fully operationalised and that this document only focuses on children and does not focus on all citizens.

Fifth, the county government also has various social media and the Governor Press Service both of which are used to proactively share information but also to respond to information requests by the citizens. The only challenge is that no data was availed on how many requests they received per year and what responses they gave.

Sixth, Makueni, is a leader in citizen participation and county government transparency, has the least information asymmetry relative to the other four counties but it also has some work to meet its full obligations under the law.

However, like the other counties in the study it also faces clear challenges. The county continues to fail to meet its obligations Section 17 (c) of the Access to Information Act that requires it to have "computerised and digitised its records and information management systems in order to facilitate efficient access to information."[286] Secondly, the county government and county assembly have not for the last five years submitted to the Commission on Administrative Justice annual reports as required by law.[287]

The County Service Board did not see themselves as having any clear obligations on data protection yet they handle personal data of each of the permanent and short-term employees hired by the County Government. These findings clearly show that there is a need to create sufficient awareness among the public officials at the county to understand that nearly all departments and sectors collect or process personal data and yet none of them have conducted any Data Protection Impact Assessment (DPIA) to understand attendant risks and how best to mitigate.

Lastly, on access to information, the Makueni County Government has set up a unique portal where it publishes its detailed public procurement information; Makueni is thus a pioneer in open contracting.

Vihiga County

First, there were 15 respondents who were citizens and 4 respondents who were county officials[288] - two each from the county assembly and the county executive. These were purposive samples.

Second, the Vihiga County government is the only one that has developed and deployed the Geographical Information System (GIS).[289] The system is used to support the implementation of the CIDP and development of sectoral plans and spatial plans. They facilitate public participation in county planning and development and promote transparency, accountability and overall governance.

Lastly, the researchers note that Vihiga has the ***Vihiga County Health Care Service Bill, 2019***[290] . Under Section 22 of the Bill, the Bill explicitly provides for Confidentiality of information for all citizens, with information being disclosed under patient's consent or under order of court or for the purpose of legal proceedings. The researchers note that this document is still a Bill and not yet an Act and thus has not been fully operationalised.

4

Conclusion and Recommendations

First, this report has documented the opportunities and challenges presented by legislation that encourages access to information and public participation against compliance with the Access to Information 2016 and the Data Protection Act 2019 at the national and county level.

Second, in some counties, citizen groups and proactive public officials are sharing information on public procurement and many other public service issues. The only challenge is that they tend to use mechanisms and platforms that reach the majority but are never tailor-made to reach the marginalised and disadvantaged groups in the communities.

Third, the level of knowledge and awareness about the information rights, especially access to information and data protection is still significantly low among citizens and public officials in the counties. Women, youth and persons with disability are disproportionately affected as their levels are very low yet with access to timely and comprehensive information their lives and life conditions would be significantly improved.

Fourth, the study finds that there is an opportunity to use data procurement data to develop affirmative actions for tenders that seek to reach the poor, youth, persons with disability and women.

Fifth, the study also reveals that data protection is quite a complex subject matter and a fairly new subject matter to the many of the counties in Kenya. It will take some time to be fully comprehended and applied by stakeholders. There is no holistic understanding of the concept of "information rights" and a full account of the notion and how it may apply to the national government and the county governments in Kenya.

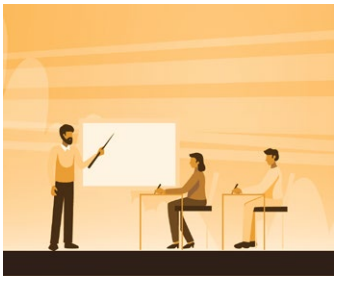
Sixth, efforts at national and county levels are fragmented and disarticulated. There is a need for an immediate effort to develop working collaboration between the two oversight mechanisms for the access to information and data protection to ensure that public bodies at national and county levels have a holistic understanding of the information rights.

Seventh, all the five counties have developed some mechanisms to implement access to information laws through various protocols, mechanisms and procedures. They have also designated information officers. However, none of the five counties studied have passed comprehensive access to information laws even though the Model Law on Access to Information was developed by the Commission on Administrative Justice.

Eighth, the five sub nationals have designated some officers to assist in facilitating access to information. These officers largely are trained journalists and communication experts. There is a need to bolster the respective departments with data scientists to help augment the functions of managing information and data in ways that adhere to internationally accepted fair information practices.

Lastly, County governments have an obligation to facilitate the realisation of information rights of its citizenry even as they ensure they have requisite information management systems that ensure that personal and sensitive personal information collected, processed, stored and transferred is managed in ways that respect and meet the fair information principles.

The study makes the following recommendations:

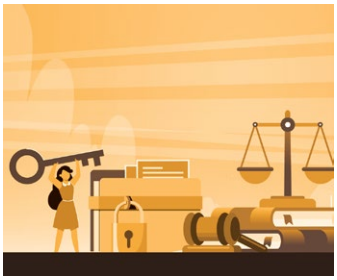


Capacity Building for citizens/community groups and public officers

There is a clear need for the development and implementation of a targeted county public awareness and education programme on information rights. The programme should be able to show the complementarity and conflict between the right to access to information and the right to privacy in general and data protection rights in particular. We note that in October 2021 the Office of the Data Protection Commissioner released its draft strategic plan[291] that prioritizes creating awareness on Data Protection. However, the plan doesn't specifically consider access to information aspects and fails to address the complementarity and conflict between access to information and the right to privacy.

Support counties to make annual reports to the Commission on Administrative Justice

All the counties studied have not submitted a single annual report to the Commission on Administrative Justice since 2016. Preparation and submission of the annual reports would serve two purpose: meeting their legal obligations pursuant to Section 27 of the Access to Information Act, 2016; and enabling the county to reflect and understand what is working and what changes they ought to initiate to meet fulfil their legal obligations and be accessible and accountable to their diverse communities of their populations. We note that the ODPC Draft strategic plan[292] aims to set up regional officers in 12 clusters across the country to be responsible for data protection in the counties. We recommend that such offices be mandated to coordinate with counties and make reports on data protection to the ODPC highlighting the intersections with access to information.



Develop and adopt clear and comprehensive access to information and data protection policies and legislations

County governments should establish policy, legislative and institutional frameworks to facilitate effective and timely access to information and data protection in all their administrative and service provision processes. They should also develop and resource all institutional and administrative frameworks up to sub-ward levels and ensure that they proactively disclose information within the confines of the Access to Information 2016.

Build the capacity of counties to undertake Data Protection Impact Assessment

National government and counties have run COVID-19 relief subsidies programmes among many other programmes where they collected and processed personal information and sensitive personal information. However, none of the counties in the study, nor the national government, have undertaken any DPIA yet it is a minimum requirement before any programme especially if such a project is likely to "high risk" to other people's personal information.

Undertaking a timely and comprehensive DPIA is one way in which County Governments can readily demonstrate to the oversight mechanism (Office of the Data Protection Commissioner) that they comply with the Data Protection Act, 2019. This situation may be attributed to the fact that all the five counties did not have any data scientists and experts on data protection and security in their stables as they may not have fully recognised their obligations under the Data Protection Act, 2019. We also note that the ODPC has a released a guidance note on conducting a Data protection impact assessment that offers valuable information on processing operations where a DPIA is required and the procedure to be followed when conducting a DPIA[293].

A credible DPIA must contain the following elements:

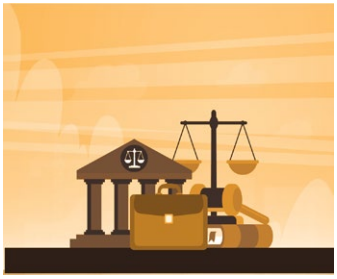
1. A systematic description of the envisaged processing operations and purposes of processing, including where applicable, the legitimate interest pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. An assessment of the risks to the rights and freedoms of data subjects; and
4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure protection of personal data and to demonstrate compliance with the DPA.

Hire and train dedicated Data Protection Officers

County governments process a number of different data sets of personal data that require qualified and dedicated Data Protection Officers to ensure they safeguard them and remain in compliance with the DPA. This must therefore be a minimum requirement for all counties. County governments should create financial resource measures to ensure that the office of the data protection authority is able to operate with offices in each county. Once data protection officers are hired, counties could work with the Office of the Data Protection Commissioner to develop tailor-made training and certification programmes. This would help the ODPC meet the objectives of its strategic plan with optimum utilization of public finances as hiring of staff by the ODPC heavily relies on budgetary allocations.

Strengthen civil society organisations information rights and data governance programmes

Civil Society Organisations (CSOs) play a critical role in ensuring citizen-agency and county governments should take advantage of the social capital, skills, knowledge in CSOs to establish the mechanisms for interaction and co-learning to ensure better data governance practices that ensure data justice to all. CSOs working at the national and county levels should deepen and strengthen their programmes on information rights. They should engage with the national and county governments to ensure compliance with international human rights standards, including the UN Guiding Principles on Business. The draft strategic plan recognises CSOs as important stakeholders who champion for protection of vulnerable groups and information sharing. The ODPC expects that CSOs will contribute heavily with promoting awareness of data protection and compliance with the data protection Act.



To the private sector at the national and county levels

1. Carry out a Data Protection Impact Assessment to ensure that all data collected is in strict compliance with the three-part test under international human rights law, and data protection principles, including data minimisation and privacy by design.These entities are encouraged to rely on the guidance note on DPIA issued by the ODPC.
2. Engage with the national and county governments to ensure compliance with international human rights standards, including the UN Guiding Principles on Business and Human Rights, and national laws protecting the rights to privacy, and access to information.

Protecting data rights of children

There is a need to undertake further research on how data protection and information rights affect children and their rights. This is very significant because children are less able to fully understand the implications of their rights to privacy and often do not have the opportunities or power to communicate their opinions[294]. Children also often lack the resources to respond to instances of bias or to rectify any misconceptions in their data; and it is often the case that national statutes and regulations (in fact the DPA 2019 mentions children only once) including ethical guidelines rarely speak to the needs of children. Whereas this is out of scope for this study, it is recommended that more research is undertaken to generate evidence in this particular area for policy development. The draft ODPC strategic plan proposes to create the Legal and Advisory Directorate within its governance structure to be responsible for handling children's data protection rights.

APPENDIX

Structured Questionnaire – Citizens and CSOs

1. How long have you been residing in this county?

A. 6 months or less B. Between 1 and five years C. For more than 10 years

2. How would you describe yourself?

A. An actively engaged citizen who regularly participates in County Government decision-making processes

B. A moderately engaged citizen who participates once in a while in County Government decision making processes

C. An enlightened citizen who would want to participate in County Government decision making processes, if there was an opportunity to do so

D. An enlightened but passive citizen with little interest in participating in County Government decision making processes

3. How involved are you in how this County is managed or governed?

A. Highly involved

B. Moderately involved

C. Hardly ever involved

D. Not involved at all

4. How would you describe your engagement with the County Government? (Tick as many as appropriate

A. I regularly make demands on County Government officials to make public the information they have, which might be of public interest

B. I have had frequent confrontations with the County Government over its policies

C. The County Government uses its public participation forums to rubber stamp decisions that were made elsewhere; I avoid these platforms because they add little value.

D. I am a passionate participant at the County public participation forums, since I use them to hold County Government officials accountable for their actions

5. Have you ever requested or demanded information from this County Government?

A. Yes B. No (if No, skip to question 8)

6. In what area was the information you requested or demanded from the County Government? Tick as many as appropriate

A. Procurement

B. County budgetary allocations

C. Financial/expenditure statements

D. Development plans

E. Other (please specify)

7. Were you able to get the information you requested or demanded from the County Government?

A. Yes B. No

8. Have you ever been invited to participate in decision making involving an activity by the County Government?

A. Yes B. No (if No, skip to Question 11)

9. In what activity were you invited to participate?

A. Call for procurement of goods and services

B. Public hearing on County budgetary allocations

C. Public hearing on financial/expenditure statements

D. Public participation in preparation of County development plans

E. Other (please specify)

10. How many times have you been invited to participate in a decision making process organized by the County Government in the last six months?

A. Once B. Twice C. More than five times D. Can't recall

11. How would you rate your ability to influence the decisions of the County Government?

A. Very High

B. Moderate

C. Very Low

D. Don't know

12. How would you rate your ability to demand information from the County Government?

A. Very High

B. Moderate

C. Very Low

D. Don't know

13. Do you know of instances where the County Government has collected personal data of citizens?

A. Yes B. No

14. How is such data normally collected? Tick as many as appropriate

A. When registering for County Government services

B. When making payments for County Government services

C. During visits to County Government services

D. Other (please specify)

15. How confident are you that the personal data collected by the County Government is secure from abuse, or unauthorized use?

A. Very confident

B. Slightly confident

C. Not confident at all

D. Don't know

REFERENCES

1 Turkel, E. and Turkel, G. (2016). *Public Value Theory: Reconciling Public Interests, Administrative Autonomy and Efficiency*. Review of Public Administration and Management. <https://www.longdom.org/open-access/public-value-theory-reconciling-public-interests-administrativeautonomy-and-efficiency-2315-7844-1000189.pdf> accessed on 18 August 2021

2 Article 31 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

3 Article 33 and 34 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

4 Article 35 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

5 Murdock, G. 2004. Building the Digital Commons: Public Broadcasting in the age of the Internet. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.627.2917&rep=rep1&type=pdf> accessed 18 August 2021

6 Intergovernmental Relations Technical Committee, The Status Of Public Participation In National And County Governments <https://countytoolkit.devolution.go.ke/sites/default/files/resources/27.%20The%20Status%20of%20Public%20Participation%20in%20National%20and%20County%20Governments%20.pdf> accessed 18 August 2021

7 Philip Coppel, Information Rights: *Law and Practice* (3rd edition, Hart Publishing 2010) l

8 ARTICLE 19, Access to Information: An Instrumental Right for Empowerment, 2007 <https://www.article19.org/data/files/pdfs/publications/ati-empowerment-right.pdf > accessed 18 August 2021

9 ICJ Kenya in June 2021 called for an expression of interest to support the production of the inaugural annual report. See < https://icj-kenya.org/?post_type=job_listing&p=5787> accessed 18 August 2021

10 Kenya's Fourth National Action Plan 2020-2022: <https://www.opengovpartnership.org/documents/kenya-action-plan-2020-2022/> accessed 18 August 2021

11 OGP Local members. See < https://www.opengovpartnership.org/ogp-local/ >accessed 18 August 2021

12 OGP, Kenya Design report 2018-2020 < https://www.opengovpartnership.org/documents/kenya-design-report-2018-2020/> accessed 18 August 2021

13 Commission on Administrative Justice, Draft Specimen Model Law on Access to Information, <https://www.ombudsman.go.ke/index.php/access-to-information-centre/category/84-draft-specimen-model-law-on-access-to-information> accessed 18 August 2021 and Commission on Administrative Justice, Handbook on Best Practices on Implementation of Access to Information in Kenya 2018, <https://countytoolkit.devolution.go.ke/sites/default/files/resources/Handbook%20on%20Best%20Practices%20on%20Implementation%20of%20Access%20to%20Information%20in%20Kenya.pdf> accessed 18 August 2021

14 Interview with Ms Florence Kajuju, Chairperson, Commission on Administrative Justice, 10 July 2021

15 Interview with Ms Lucy Ndung'u, Access to Information Commissioner, CAJ, on 10 July 2021

16 *Kenya: The Access to Information Regulations,* 2021 [Kenya], <http://www.okoamombasa.org/wp-content/uploads/2021/06/ATI-REGULATIONS-2021-FOR-PUBIC-PARTICIPATION-25-05-2021.pdf> accessed 18 August 2021

17 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 18 August 2021

18 The Universal Declaration of Human Rights is not a treaty to which states become parties by signing the document, but is considered an authoritative universally accepted statement on human rights that states must adhere to.

19 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 18 August 2021

20 University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <http://hrlibrary.umn.edu/research/ratification-kenya.html> accessed 18 August 2021

21 UN Human Rights Committee (HRC), General Comment No.34: *Article 19: Freedoms of opinion and expression*, 21 July 2011, < https://www.refworld.org/docid/4e38efb52.html>accessed 18 August 2021

22 Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights ("Banjul Charter")*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), <https://www.refworld.org/docid/3ae6b3630.html> accessed 18 August 2021

23 University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <http://hrlibrary.umn.edu/research/ratification-kenya.html> accessed 18 August 2021

24 Kariuki,Othero et al, 'Legal Alert:Kenya Data Commissioner issues new Draft Data Protection (General Regulations) 2021' (TripleOKLaw, 19 April 2021) <https://tripleoklaw.com/kenyan-draft-data-protection-general-regulations/> accessed 18 August 2021

25 *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679> accessed 18 August 2021

26 UN General Assembly, U*niversal Declaration of Human Rights,* 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 18 August 2021

27 The Universal Declaration of Human Rights is not a treaty to which states become parties by signing the document, but is considered an authoritative universally accepted statement on human rights that states must adhere to.

28 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 18 August 2021

29 University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <http://hrlibrary.umn.edu/research/ratification-kenya.html> accessed 18 August 2021

30 UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988<https://www.refworld.org/docid/453883f922.html>accessed 18 August 2021

31 Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights ("Banjul Charter")*, 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), <https://www.refworld.org/docid/3ae6b3630.html> accessed 18 August 2021

32 Ivan Stepanov, "Introducing a Property Right over Data in the EU: the Data Producer's Right- an evaluation" (2019) Vol. 34 International Review of Law, Computers and Technology, <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621> accessed 18 August 2021

33 Atul Singh, "Protecting Personal Data as a Property Right" (2016) ILI Law Review <https://ili.ac.in/pdf/p9_atul.pdf> accessed 18 August 2021

34 University of Minnesota Human Rights Library, 'Ratification of International Human Rights Treaties - Kenya' <http://hrlibrary.umn.edu/research/ratification-kenya.html> accessed 18 August 2021

35 African Union, *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014, < https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 18 August 2021

36 African Union, *African Union Convention on Cyber Security and Personal Data Protection Status List*, <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 18 August 2021

37 African Commission on Human and People's Rights, *African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa* <https://www.achpr.org/legalinstruments/detail?id=69> accessed 18 August 2021

38 United Nations, *Guiding Principles on Business and Human Rights* <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 18 August 2021

39 Internet Rights and Principles Dynamic Coalition, 10 Internet Rights and Principles (Internet Rights and Principles Dynamic Coalition) <http://internetrightsandprinciples.org/site/charter/> accessed 18 August 2021

40 United Nations, *Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6 (rev. 1)-E). Second Phase of the WSIS (16-18 November 2005, Tunis).* <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> accessed 18 August 2021

41 OECD, *Seoul Declaration for the Future of the Internet Economy, June 18, 2008*, <http://itlaw.wikia.com/wiki/Seoul_Declaration_for_the_Future_of_the_Internet_Economy> accessed 18 August 2021

42 OECD, 'Kenya becomes the 94th jurisdiction to join the most powerful multilateral instrument against offshore tax evasion and avoidance' <https://www.oecd.org/ctp/exchange-of-tax-information/kenya-becomes-the94th-jurisdiction-to-sign-the-mac.htm> accessed 18 August 2021

43 NETmundial Multistakeholder Statement. April, 24th 2014 <http://netmundial.br/netmundial-multistakeholder-statement/> accessed 18 August 2021

44 United Nations, Resolution on "*the right to privacy in the digital age*" *(A/HRC/34/L.7/Rev.1)*, <https://www.article19.org/data/files/HRC.34.L.7.Rev1_Privacy_in_the_digital_age_1.pdf> accessed 18 August 2021

45 ARTICLE 19, 'UN HRC: Resolution on Safety of Journalists Breaks New Ground' (ARTICLE 19 Website, 29 September 2016) <https://www.article19.org/resources.php/resource/38504/en/un-hrc:-resolution-on-safety-of-journalists-breaks-new-ground> accessed 18 August 2021

46 ARTICLE 19, 'UN expert launches robust defence of online anonymity and encryption' (ARTICLE 19 Website, 28 May 2015) <https://www.article19.org/resources.php/resource/37979/en/un-expert-launches-robust-defence-of-online-anonymity-and-encryption> accessed 18 August 2021

47 African Commission on Human and Peoples Rights, 362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016, <https://www.achpr.org/sessions/resolutions?id=374> accessed 18 August 2021

48 "African Declaration on Internet Rights and Freedoms," African Declaration Coalition, last modified on August 5, 2015, <https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf> accessed 18 August 2021

49 International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 18 August 2021

50 David Kaye, 'Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,' <www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc> accessed 18 August 2021

51 Report of the High Commissioner for Human Rights on the right to privacy in the digital age A/HRC/27/37 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 18 August 2021

52 European Parliament, *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))* <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN>accessed 18 August 2021

53 European Commission, *Report on the democratic Oversight of the security services and report on the democratic oversight of Signals Intelligence Agencies* <http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e> accessed 18 August 2021

54 ARTICLE 19, *The Global Principles on Protection of Freedom of Expression and Privacy* <https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf> accessed 18 August 2021

55 Republic of Kenya, *Digital Economy Blueprint, Powering Kenya's transformation*, <https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf> accessed 18 August 2021

56 Republic of Kenya, *Emerging Digital Technologies for Kenya, Exploration and Analysis* (Ministry of Information, communication and Technology, July 2019) <https://www.ict.go.ke/blockchain.pdf> accessed 18 August 2021

57 Republic of Kenya, *Digital Economy Blueprint, Powering Kenya's transformation*, <https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf> accessed 18 August 2021

58 The World Bank, World Development Report 2021: Data for better lives, <https://wdr2021.worldbank.org/the-report/> accessed 18 August 2021

59 See Article 174 of the Kenya: *The Constitution of Kenya, 2010* [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

60 Cyrus Farivar, *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (Melville House, 2018), Cyrus Farivar, 2018. Privacy Vs The Rise of Surveillance Tech, Melville House. See also Daniel J. Solove and Paul M. Schwartz, *Consumer Privacy and Data Protection* (3rd edn, Wolters Kluwer 2020)

61 David Banisar, *The Right to Information and Privacy: Balancing and Managing Conflicts*, The World Bank 2011, <https://openknowledge.worldbank.org/handle/10986/23022> accessed 18 August 2021

62 See Section 26 of the Kenya: *Data Protection Act, No 24 of 2019* [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

63 See s. 4(1) and S. 6 (1) (d) of the Kenya: *Access to Information Act, No 31 of 2016* [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

64 See s. 26 (b), (d), & (e) of the Kenya: *Data Protection Act, No 24 of 2019* [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021 and S. 13 (1) Kenya: *Access to Information Act, No 31 of 2016* [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

65 See examples, David Mwere, 'Agency pledges action after complaints over political parties 'Data Breach" (Daily Nation, June 26 June 2021) <https://nation.africa/kenya/news/agency-pledges-action-after-complaints-over-political-parties-data-breach--3450886?fbclid=IwAR12YC2h8PYCbvBNliwVXCJB_dnSETU5pArDoz_dTGWz0-VslRcp_6bnwjY>accessed 18 August 2021; and ShahidiNews Team, 'Lobby Group calls for investigations over breach of personal data by political parties,' (Shahidi News, June 22,2021) <https://shahidinews.co.ke/2021/06/22/lobby-group-calls-for-investigations-over-breach-of-personal-data-by-political-parties/> accessed 18 August 2021

66 Nixon Kanali, 'Digital lenders in Kenya are still abusing data protection laws.' (*TechTrendsKe* 3 June 2021) <https://techtrendske.co.ke/digital-lenders-in-kenya-are-still-abusing-data-protection-laws/> accessed 18 August 2021

67 See among others Guerra and Others v. Italy, European Court of Human Rights, 116/1996/735/932, February 19,1998; Hencke, David. 2001. "MP Challenges Secrecy Culture." The Guardian, 27 June 2021. Available at <https://www.theguardian.com/politics/2001/jun/27/freedomofinformation.uk> accessed 18 August 2021

68 Daily Mail, 2006. 'Anger as Police Obtain Journalist's Mobile Records to Discover Source.' (Daily Mail, 1 December 2006) <https://www.dailymail.co.uk/news/article-419986/Anger-police-obtain-journalists-mobile-records-discover-source.html> accessed 18 August 2021

69 Chintan Gurjar, Case Study- News of the World phone hacking scandal. (Infosec, 3 April 2014) <https://resources.infosecinstitute.com/topic/case-study-news-world-phone-hacking-scandal-notw/> accessed 18 August 2021

70 See EPIC v DHS (suspension of Body Scanner Program), <https://epic.org/privacy/litigation/apa/tsa/bodyscanner/> accessed 18 August 2021 ; EFF (2010); and ACLU, <https://www.aclu.org/> accessed 18 August 2021

71 Defenders Coalition, 'Perception Survey Report: The Impact of Communication Surveillance on Human Rights Defenders in Kenya,' < https://defenderscoalition.org/4912-2/> accessed 18 August 2021

72 Charmz, K., & Belgrave, L.L.2015. *Grounded Theory*. The Blackwell Encyclopedia of Sociology.

73 Ibid, PP3-6

74 The ruling party Jubilee won 25 gubernatorial seats, ODM won 13. Wiper Democratic Movement-Kenya like Ford-Kenya won two of the seats. Two other governors won their seats as independents while National Rainbow Coalition, Maendeleo Chap Chap, KANU won one seat each.

75 Infotrak 2020, 'Governors Approval Rating' <http://countytrak.infotrakresearch.com/governors-approval-rating/> accessed 18 August 2021

76 Alt, J. E., Dreyer, D. L. and Skilling, D. (2002). Fiscal Transparency, Gubernatorial Approval, and the Scale of Government: Evidence from the States. State Politics & Policy Quarterly. Vol 2(3). pp 230-250

77 Infotrak, 2020. 'Countytrak Index by Regions,' <http://countytrak.infotrakresearch.com/index-by-regions/> accessed 18 August 2021

78 IBP, 2019. 'Open Budget survey,' <https://internationalbudget.org/kenya-county-budget-transparency-survey-2019/> accessed 18 August 2021

79 IBP, 2019. 'Open Budget survey,' <https://internationalbudget.org/kenya-county-budget-transparency-survey-2019/> accessed 18 August 2021

80 Special Audit Report of the Auditor-General on Utilization of Covid-19 Funds by County Governments, December 2020

81 Special Audit Report of the Auditor-General on Utilization of Covid-19 Funds by County Governments, December 2020, see specifically Bomet (pages 70-80); kilifi (pages 228-232); Makueni (pages 348-364), Taita Taveta (pages 529-549) and Vihiga (pages 608-618).

82 See Art 2(6) of the Kenya: *The Constitution of Kenya*, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

83 UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 18 August 2021

84 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 18 August 2021

85 See Art 12 of the UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 18 August 2021

86 See Art 17 of the UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 18 August 2021

87 See Art 35 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

88 Ibid, Art 33 (1)(a)

89 Ibid, Art 10(2)

90 Ibid, Art 232(1)(f)

91 Global RTI Ranking, <https://www.rti-rating.org/country-data/> accessed 18 August 2021

92 ibid

93 S.20-24 of the Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

94 S 3 of of the Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

95 Ibid, Part II

96 Ibid, s 5

97 Ibid, s 6(1)

98 Ibid, s 6(2)

99 Ibid, s 7

100 Ibid, s 9; s 10.

101 Ibid, s 11(1)

102 Ibid, s 12

103 Ibid, s 9

104 Ibid, s 13

105 Ibid, s 14

106 Ibid, s 16

107 Ibid, s 17

108 Ibid, s 18

109 Ibid, s 25

110 Ibid, s 26

111 Ibid, s 27

112 Ibid, s 28

113 Commission on Administrative Justice, *Draft Specimen Model Law on Access to Information*, <https://www.ombudsman.go.ke/index.php/access-to-information-centre/category/84-draft-specimen-model-law-on-access-to-information> accessed 18 August 2021 and Commission on Administrative Justice, *Handbook on Best Practices on Implementation of Access to Information in Kenya 2018*, <https://countytoolkit.devolution.go.ke/sites/default/files/resources/Handbook%20on%20Best%20Practices%20on%20Implementation%20of%20Access%20to%20Information%20in%20Kenya.pdf> accessed 18 August 2021

114 Interview with Ms Florence Kajuju, Chairperson, Commission on Administrative Justice, 10 July 2021

115 Interview with Ms Lucy Ndung'u, Access to Information Commissioner, CAJ, on 10 July 2021

116 Commission on Administrative Justice, New Strategic Plan Launched, <https://www.ombudsman.go.ke/index.php/launch-of-the-second-strategic-plan-2019-2023> accessed 18 August 2021

117 Interview with Ms Lucy Ndung'u, the Access to Information Commissioner, on 10 July 2021

118 Kenya: The *Access to Information Regulations, 2021* [Kenya], <http://www.okoamombasa.org/wp-content/uploads/2021/06/ATI-REGULATIONS-2021-FOR-PUBIC-PARTICIPATION-25-05-2021.pdf> accessed 18 August 2021

119 Office of the President, Executive Order No 2 of 2018, <https://s3-eu-west-1.amazonaws.com/s3.sourceafrica.net/documents/118382/Executive-Order-No-2-of-2018-Procurement-of.pdf> accessed 18 August 2021

120 Andrew Omtatah Okoiti V Attorney General & 2 others [2011] eKLR <http://kenyalaw.org/caselaw/cases/view/77358> accessed 18 August 2021

121 Kahindi Lekalhaile & 4 others v Inspector General National Police Service & 3 others [2013] eKLR <http://kenyalaw.org/caselaw/cases/view/92539> accessed 18 August 2021

122 Famy Care Limited v Public Procurement Administrative Review Board & Another & 4 others [2013]eKLR <http://kenyalaw.org/caselaw/cases/view/88265> accessed 18 August 2021

123 Nairobi Law Monthly Company Limited V Kenya Electricity Generating Company & 2 Others [2013] eKLR <http://kenyalaw.org/caselaw/cases/view/88569/> accessed 18 August 2021

124 Katiba Institute v President's Delivery Unit & 3 others [2017] eKLR <http://kenyalaw.org/caselaw/cases/view/144012/> accessed 18 August 2021

125 Nelson O Kadison v Advocates Complaints Commission & another [2013] eKLR <http://kenyalaw.org/caselaw/cases/view/93012> accessed 18 August 2021

126 John Harun Mwau v Linus Gitahi & 13 others [2016] eKLR <http://kenyalaw.org/caselaw/cases/view/119817/> accessed 18 August 2021

127 Trusted Society of Human Rights Alliance & 3 others v Judicial Service Commission & another [2016] eKLR <http://kenyalaw.org/caselaw/cases/view/125135/> accessed 18 August 2021

128 See Section 3 of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

129 See Article 31 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

130 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679> accessed 18 August 2021

131 See Section 4(a) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

132 Laura Hoffman, Kenya Data Protection Act of 2019 | Summary, 5 February 2020

<https://www.michalsons.com/blog/kenya-data-protection-act-of-2019/41677> accessed 18 August 2021

133 See PArt IV of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

134 See Section 26(a) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

135 See Section 26(b) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

136 See Section 26(c) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

137 See Section 26(d) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

138 See Section 26(e) of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

139 Deloitte, Kenya Data Protection Act: A Quick Guide, 2021 <https://www2.deloitte.com/content/dam/Deloitte/ke/Documents/risk/Kenya%20Data%20Protection%20Act%20-%20Quick%20Guide%202021.pdf> accessed 18 August 2021

140 Golla, Sebastian J. "Is data protection law growing teeth: The current lack of sanctions in data protection law and administrative fines under the GDPR." J. Intell. Prop. Info. Tech. & Elec. Com. L. 8 (2017): 70.

141 Dr. Isaac Rutenberg, Expert Commentary: Kenya follows the path of European-style Data Protection, World Privacy Forum, 22 November, 2019 <https://www.worldprivacyforum.org/2019/11/expert-commentary-kenya-follows-the-path-of-european-style-data-protection/> accessed 18 August 2021

142 Eline Chivot and Daniel Castro, GDPR Penalties Prove Why Compliance Isn't Enough—And Why Companies Need Clarity, 8 May 2019 <https://itif.org/publications/2019/05/08/gdpr-penalties-prove-why-compliance-isnt-enough-why-companies-need> accessed 18 August 2021

143 Kenya: The Registration of Persons (National Integrated Identity Management System) Rules, 2020 [Kenya], <https://www.hudumanamba.go.ke/wp-content/uploads/2021/05/THE-REGISTRATION-OF-PERSONS-NATIONAL-INTEGRATED-IDENTITY-MANAGEMENT-SYSTEM-REGULATIONS-2020.pdf> accessed 18 August 2021

144 Petition 56,58 & 59 [Consolidated] Nubian Rights Forum and 2 others v. Attorney General & 6 others; Child Welfare Society & 9 Others,<http://kenyalaw.org/caselaw/cases/view/189189/> accessed 18 August 2021

145 ODPC, Citizen's Service Charter for the Office of the ODPC 2021, <https://www.odpc.go.ke/download/odpc-charter/?wpdmdl=7622&refresh=614c7832eb6be1632401458> accessed 18 August 2021

146 ODPC, Complaints Handling Manual 2021, <https://www.odpc.go.ke/download/odpc-complaints/?wpdmdl=7624&refresh=614c7832eae801632401458> accessed 18 August 2021

147 Kenya: Huduma Namba Regulations, 2020 [Kenya], <https://www.odpc.go.ke/download/huduma-namba-regulations2021/?wpdmdl=8123&refresh=614c7bb023fba1632402352> accessed 18 August 2021

148 Kenya: *Registration of Data Controllers and Processors Regulation 2021* [Kenya], <https://www.odpc.go.ke/wp-content/uploads/2021/05/Data-Protection-Registration-of-data-controllers-and-data-processor-Regulations.pdf> accessed 18 August 2021

149 Kenya: Data Protection *(compliance and Enforcement) Regulations, 2021* [Kenya],

<https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/> accessed 18 August 2021

150 Kenya: ODPC Guidance Note on Consent, 2021 [Kenya] <https://www.odpc.go.ke/download/odpc-consent/?wpdmdl=7626&refresh=614c790d959061632401677> accessed 18 August 2021

151 Interview with Victor Ndede and Demas Kiprono, Programme Officers, Amnesty International-Kenya, August 2021

152 Interview with DPC, Immaculate Kasait, 19 August 2021

153 Njeri Wangari, 'Kenya Must Implement Data Protection Law Before 2022 Presidential Election,' (Global Voices, 16 January 2021)

<https://globalvoices.org/2021/01/16/kenya-must-implement-data-protection-law-before-2022-presidential-election/> accessed 18 August 2021

154 Privacy International, Analysis of Kenya's Data Protection Act, 2019

<https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf> accessed 18 August 2021

155 s 28 of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

156 s 30 of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

157 Citizen Information, 'Surveillance in the workplace' <https://www.citizensinformation.ie/en/employment/employment_rights_and_conditions/data_protection_at_work/surveillance_of_electronic_communications_in_the_workplace.html#:~:text=Reasonable%20and%20unreasonable%20use%20of,if%20using%20CCTV%20is%20reasonable.&text=However%2C%20using%20CCTV%20to%20constantly,be%20justified%20in%20special%20circumstances.> accessed 18 August 2021

158 s36 of the Kenya: Data Protection Act, No 24 of 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf> accessed 18 August 2021

159 Regulation 7 of the Kenya: The Draft Data Protection Act (General) Regulations 2021, [Kenya] <https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf> accessed 18 August 2021

160 Kenya: Legal Notice 130, Land Registration (electronic transactions) Regulations 2020, second Schedule [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2020/LN130_2020.pdf> accessed 18 August 2021

161 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others* (Interested Parties) [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/189189/> accessed 18 August 2021

162 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), <https://www.refworld.org/docid/3ae6b3712c.html> accessed 18 August 2021

163 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, <https://www.refworld.org/docid/3ae6b3aa0.html> accessed 18 August 2021

164 Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), <https://www.refworld.org/docid/3ae6b3630.html> accessed 18 August 2021

165 African Union, African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014, < https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 18 August 2021

166 African Commission on Human and People's Rights, African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa <https://www.achpr.org/legalinstruments/detail?id=69> accessed 18 August 2021

167 United Nations, Guiding Principles on Business and Human Rights <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 18 August 2021

168 United Nations, Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6 (rev. 1)-E). Second Phase of the WSIS (16-18 November 2005, Tunis). <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> accessed 18 August 2021

169 OECD, Seoul Declaration for the Future of the Internet Economy, June 18, 2008, <http://itlaw.wikia.com/wiki/Seoul_Declaration_for_the_Future_of_the_Internet_Economy> accessed 18 August 2021

170 Internet Rights and Principles Dynamic Coalition, 10 Internet Rights and Principles (Internet Rights and Principles Dynamic Coalition) <http://internetrightsandprinciples.org/site/charter/> accessed 18 August 2021

171 NETmundial Multistakeholder Statement. April, 24th 2014 <http://netmundial.br/netmundial-multistakeholder-statement/> accessed 18 August 2021

172 United Nations, Resolution on "the right to privacy in the digital age" (A/HRC/34/L.7/Rev.1), <https://www.article19.org/data/files/HRC.34.L.7.Rev1_Privacy_in_the_digital_age_1.pdf> accessed 18 August 2021

173 African Commission on Human and Peoples Rights, 362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016, <http://www.achpr.org/sessions/59th/resolutions/362/> accessed 18 August 2021

174 "African Declaration on Internet Rights and Freedoms," African Declaration Coalition, last modified on August 5, 2015, <http://africaninternetrights.org/declaration-container/declaration/> accessed 18 August 2021

175 International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 18 August 2021

176 ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy <https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf> accessed 18 August 2021

177 Okiya Omtatah Okoiti & 2 others v Attorney General & 3 others [2014] eKLR <http://kenyalaw.org/caselaw/cases/view/103808/> accessed 18 August 2021

178 International Principles on the Application of Human Rights to Communications Surveillance (May 2014) <https://en.necessaryandproportionate.org/> accessed 18 August 2021

179 Samson Mumo Mutinda v Inspector General National Police Service & 4 others [2014] eKLR: <http://kenyalaw.org/caselaw/cases/view/94430/> accessed 18 August 2021

180 Petition No. 503 of 2014, Bernard Murage v Finserve Africa Limited & 3 others [2015] eKLR

< http://kenyalaw.org/caselaw/cases/view/109772> accessed 18 August 2021

181 Bernard Murage v Fineserve Africa Limited & 3 others [2015] eKLR <http://kenyalaw.org/caselaw/cases/view/109772/> accessed 18 August 2021

182 Case of J W I & another v Standard Group Limited & another [2015] eKLR : <http://kenyalaw.org/caselaw/cases/view/110478/> accessed 18 August 2021

183 David vs. Goliath fight in KPMG employee phone hacking case

<https://businesstoday.co.ke/david-vs-goliath-battle-in-kpmg-employee-phone-hacking-case-2/> accessed 18 August 2021 and Gloria Jepkurui Koima & another v KPMG Advisory Services Limited & 4 others [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/188773> accessed 18 August 2021

184 Section 3(4) of Kenya: Consumer Protection Act, 2012 [Kenya], <http://www.parliament.go.ke/sites/default/files/2017-05/ConsumerProtectionActNo46of2012.pdf> accessed 18 August 2021

185 Section 2 of of Kenya: Consumer Protection Act, 2012 [Kenya], <http://www.parliament.go.ke/sites/default/files/2017-05/ConsumerProtectionActNo46of2012.pdf> accessed 18 August 2021

186 Section 40 of of Kenya: Consumer Protection Act, 2012 [Kenya], <http://www.parliament.go.ke/sites/default/files/2017-05/ConsumerProtectionActNo46of2012.pdf> accessed 18 August 2021

187 Reel Analytics, State of Digital Lending in Kenya 2021 (August 2021) < https://www.dlak.co.ke/uploads/1/9/8/3/19835783/2021-reelanalytics-digital-lending-research-report.pdf> accessed 18 August 2021

188 ibid

189 Citizen TV, 'Debt of Shame: Unorthodox debt recovery tactics used by some digital lenders' (YouTube, 18 July 2021) < https://www.youtube.com/watch?v=D862mm4kRM4> accessed 18 August 2021

190 The National Assembly, Report on the Central Bank of Kenya (Amendment) Bill, National Assembly Bill No 10 of 2021 (Republic of Kenya, 05 August 2021) < http://www.parliament.go.ke/sites/default/files/2021-08/Report%20of%20the%20Central%20Bank%20of%20Kenya%20%28Amendment%29%20Bill%20No.%2010%2C%202021.pdf> accessed 18 August 2021

191 John Mutua, 'Digital lenders risk ban for revealing borrowers' (Business Daily, 15 October 2021) <https://www.businessdailyafrica.com/bd/economy/digital-lenders-risk-ban-revealing-borrowers-3583762> accessed 18 October 2021

192 Section 3 of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf> accessed 18 August 2021

193 Section 5B of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf> accessed 18 August 2021

194 Section 23 of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf> accessed 18 August 2021

195 Section 84J of the Kenya: Information And Communication Act, 1998- Revised Edition 2011 (2010) [Kenya], <https://www.ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf> accessed 18 August 2021

196 Communications Authority, 'Universal Access Projects' <https://www.ca.go.ke/industry/universal-access/projects/> accessed 18 August 2021

197 Communications Authority, 'The National KE-CIRT' <https://ke-cirt.go.ke/> accessed 18 August 2021

198 Communications Authority of Kenya, Draft Licensing and Shared Spectrum framework for Community Networks (Republic of Kenya, May 2021) <https://www.ca.go.ke/wp-content/uploads/2021/05/Licensing-and-Shared-Spectrum-Framework-for-Community-Networks-May-2021.docx.pdf> accessed 18 August 2021

199 Section 31 of the Draft Licensing and Shared Spectrum framework for Community Networks (Republic of Kenya, May 2021) <https://www.ca.go.ke/wp-content/uploads/2021/05/Licensing-and-Shared-Spectrum-Framework-for-Community-Networks-May-2021.docx.pdf> accessed 18 August 2021

200 Section 93 of the Draft Licensing and Shared Spectrum framework for Community Networks (Republic of Kenya, May 2021) <https://www.ca.go.ke/wp-content/uploads/2021/05/Licensing-and-Shared-Spectrum-Framework-for-Community-Networks-May-2021.docx.pdf> accessed 18 August 2021

201 Section 89 of the Draft Licensing and Shared Spectrum framework for Community Networks (Republic of Kenya, May 2021) <https://www.ca.go.ke/wp-content/uploads/2021/05/Licensing-and-Shared-Spectrum-Framework-for-Community-Networks-May-2021.docx.pdf> accessed 18 August 2021

202 Regulation 3 of the Kenya: The Kenya Information and Communication (Consumer Protection) Regulation 2010 [Kenya] <https://www.ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010-1.pdf> accessed 18 August 2021

203 Regulation 9 of the Kenya: The Kenya Information and Communication (Consumer Protection) Regulation 2010 [Kenya] <https://www.ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010-1.pdf> accessed 18 August 2021

204 Communications Authority, 'A Guide to Child Online Protection' <https://www.ca.go.ke/wp-content/uploads/2019/06/COP-Booklet.pdf> accessed 18 August 2021

205 Kenya: Finance Act, 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2019/FinanceAct_No23of2019.PDF> accessed 18 August 2021

206 Kenya: Finance Act, 2020 [Kenya], <https://www.kra.go.ke/images/publications/Finance-Act-2020.pdf> accessed 18 August 2021

207 Kenya: Finance Act, 2021 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2021/TheFinanceAct_No.8of2021.pdf> accessed 18 August 2021

208 Lynet Igadwah, 'Netflix hikes rates on inclusion of VAT tax charge' (The East African, 07 May 2021) < https://www.theeastafrican.co.ke/tea/business/netflix-rates-inclusion-of-vat-tax-charge-3391120> accessed 18 August 2021

209 RSM, Clarity on payment of Digital Service Tax following The Finance Act 2021 (August 2021) < https://www.rsm.global/kenya/insights/tax-insights/clarity-payment-digital-service-tax-following-finance-act-2021> accessed 18 August 2021

210 Albert Mwazighe, 'Excise duty on airtime rings up gloom across EA region' (The East African, 15 July 2021)

<https://www.theeastafrican.co.ke/tea/business/excise-duty-on-airtime-rings-up-gloom-across-ea-region-3473946> accessed 18 August 2021

211 Preamble of the Kenya: National Intelligence Service Act, 2012 [Kenya], <https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf> accessed 18 August 2021

212 Ibid, s 42

213 Ibid, s 36

214 Freedom House, Kenya: Freedom on the Net 2020, <https://freedomhouse.org/country/kenya/freedom-net/2020#footnote1_6pbjlr9> accessed 18 August 2021

215 Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR <http://kenyalaw.org/caselaw/cases/view/151117/> accessed 18 August 2021

216 Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others [2020] eKLR <http://kenyalaw.org/caselaw/cases/view/193383> accessed 18 August 2021

217 Kenya: Computer Misuse and Cybercrimes Act, 2018 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 18 August 2021

218 Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR, para 306 <http://kenyalaw.org/caselaw/cases/view/106083/> accessed 18 August 2021

219 Ibid, para 308

220 Ibid, para 463(c)(iv)

221 s 36 and s 37 of Kenya: National Intelligence Service Act, 2012 [Kenya], <https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf> accessed 18 August 2021

222 See preamble of the Kenya: Prevention of Terrorism Act, 2012, [Kenya] <https://issafrica.org/ctafrica/uploads/PREVENTION%20OF%20TERRORISM%20ACT.pdf> accessed 18 August 2021

223 Ibid, s 34

224 Ibid, s 35(2)

225 Ibid, s 35(3)(a)

226 Ibid, s 35(3)(b)

227 Ibid, s 35(3)(c)

228 Ibid, s 36.

229 Ibid, 36A

230 Ibid, s 41

231 Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR, para 306 <http://kenyalaw.org/caselaw/cases/view/106083/> accessed 18 August 2021

232 See s 64 (30A) (Repealed) of the Kenya: National security Laws amendment Act, 2014 [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf> accessed 18 August 2021

233 Ibid, s 64 (30F) (Repealed)

234 Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations, 2013, reg 5 <https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html> accessed 18 August 2021

235 Ibid, reg 5; 6

236 See preamble of the Kenya: Mutual Legal assistance Act, 2011, [Kenya] <http://kenyalaw.org:8181/exist/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/M/Mutual%20Legal%20Assistance%20Act%20Cap.%2075A%20-%20No.%2036%20of%202011/docs/MutualLegalAssistanceAct36of2011.pdf> accessed 18 August 2021

237 Ibid, s 5

238 Ibid, s 27

239 Ibid, s 31

240 Ibid, s 32

241 Ibid, part V

242 Ibid, s 42

243 Office of the Attorney General and Department of Justice, Requests For Mutual legal assistance In Criminal Matters -Guidance For Authorities Outside Of Kenya, 2018. <https://statelaw.go.ke/wp-content/uploads/2020/11/MLA-GUIDELINES-IN-CRIMINAL-MATTERS-FOR-AUTHORITIES-OUTSIDE-OF-KENYA.pdf> accessed 18 August 2021

244 Quarshie, Henry Osborn, and Alexander Martin-Odoom. "Fighting cybercrime in Africa." Computer Science and Engineering 2.6 (2012): 98-100.

245 Ng'ang'a, Alexander Mwaura. "Toward a regional ICT hub: Need for cyber laws in Kenya." Information Security Journal: A Global Perspective 18.1 (2009): 47-50.

246 Ibid.

247 See Section 3(d) of the Kenya :The Computer Misuse and Cybercrimes Act, No. 5 of 2018, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 18 August 2021

248 The Bloggers Association of Kenya (BAKE) v Attorney General & 3 Others, Constitutional Petition No 206 of 2018 <http://kenyalaw.org/caselaw/cases/view/159286> accessed 18 August 2021

249 Cyprian Nyakundi & another v Director of Criminal Investigations & 2 others; Victoria Commercial Bank (Interested Party), Constitutional Petition E284 of 2020 <http://kenyalaw.org/caselaw/cases/view/209135/> accessed 18 August 2021

250 Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties), Petition 56, 58 & 59 of 2019 (Consolidated) <http://kenyalaw.org/caselaw/cases/view/189189/> accessed 18 August 2021

251 Section 38 of the Kenya :The Computer Misuse and Cybercrimes Act, No. 5 of 2018, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 18 August 2021

252 Part IV of the Kenya :The Computer Misuse and Cybercrimes Act, No. 5 of 2018, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 18 August 2021

253 Part V of the Kenya :The Computer Misuse and Cybercrimes Act, No. 5 of 2018, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 18 August 2021

254 Walubengo, John, and Mercy Mutemi. 'Treatment of Kenya's internet intermediaries under the Computer Misuse and Cybercrimes Act, 2018.' The African Journal of Information and Communication 21 (2018): 1-19.

255 Preamble of the Kenya: Standards Act 2012, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/StandardsActCap496.PDF> accessed 18 August 2021

256 Ibid, Section 7

257 Ibid, Section 9(1)

258 Ibid, Section 9(2)

259 Fredrick Obura, '40 new privacy standards approved as cybercrime soars by 50 percent' (The Standard 24 May 2021)<https://www.standardmedia.co.ke/business/sci-tech/article/2001413799/40-new-privacy-standards-approved-as-cybercrime-cases-soar-50-per-cent>- accessed 18 August 2021

260 Kenya: Kenya Bureau of Standards Access to Information Policy 2019 [Kenya] -<https://www.kebs.org/images/CustomerCare/KEBS-ACCESS-TO-INFORMATION-POLICY.pdf>- accessed 18 August 2021

261 See Section 8 of the of the Kenya: Standards Act 2012, [Kenya] <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/StandardsActCap496.PDF> accessed 18 August 2021

262 See preamble of the Kenya: County Governments Act, No 17 of 2012, [Kenya] <http://www.parliament.go.ke/sites/default/files/2017-05/CountyGovernmentsAct_No17of2012.pdf> accessed 18 August 2021

263 Ibid, Section 96(1)

264 Ibid, No 17 of 2012, Section 96(2)

265 Ibid, Section 96(3)

266 Ibid, Section 95

267 ACHPR Observer reference number 434, A Shadow report on freedom of information in Kenya, prepared by The Africa Freedom of Information Centre in consultation with ARTICLE 19 East and Horn of Africa and the International Commission of Jurists- Kenya, Kampala Uganda, 2015, 10

268 See Section 87 of the Kenya: County Governments Act, No 17 of 2012, [Kenya] <http://www.parliament.go.ke/sites/default/files/2017-05/CountyGovernmentsAct_No17of2012.pdf> accessed 18 August 2021

269 See Article 196 of the Kenya: The Constitution of Kenya, 2010 [Kenya], 27 August 2010,<https://www.refworld.org/docid/4c8508822.html> accessed 18 August 2021

270 Interviews with County Officials took place between 12th and 23rd of July, 2021.

271 Kenya: Taita Taveta County Health Services Bill, 2020 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2020/TaitaTavetaCountyHealthServicesBill2020.pdf> accessed 18 August 2021

272 Interview with one of the Business community representatives during the Focused Group Discussion occurred in varied dates between 6th to 12th July, 2021

273 Deputy County Assembly Clerk, Taita Taveta County Assembly occured on varied dates between 13th to 23rd July, 2021.

274 Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

275 See Section 27 of the Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

276 Interview with Wallace Mwaluma, Taita Taveta County Director of Gender occured on 13th July, 2021

277 Interviews occurred on varied dates between 6th to 12th July, 2021

278 Kenya: Kilifi County Maternal, Newborn and Child Health Act, 2016 [Kenya], <https://www.kilifi.go.ke/lib.php?com=5&res_id=567#:~:text=AN%20ACT%20of%20the%20Kilifi,connected%20therewith%20and%20incidental%20thereto.> accessed 18 August 2021

279 Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

280 See Section 27 of the Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

281 Interview occurred on 13th July, 2021

282 Makueni County Government, Makueni County Public Participation Framework, <https://makueni.go.ke/public-participation-framework/> accessed 18 August 2021

283 Interviews with County Officials occured between 15th and 23rd July, 2021

284 Makueni county Government, County Disclosure and Communication Policy

285 Kenya: Makueni County Maternal, Newborn and Child Health Bill, 2017 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/MakueniCountyMaternalNewbornandChildHealthBill2017.pdf> accessed 18 August 2021

286 Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

287 See Section 27 of the Kenya: Access to Information Act, No 31 of 2016 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/AccesstoInformationActNo31of2016.pdf> accessed 18 August 2021

288 Interview dates varied from 19th to 30th July, 2021

289 Vihiga County, Establishment of Geographic Information System in the County Government of Vihiga, <https://locateit.co.ke/establishment-of-geographic-information-system-in-the-county-government-of-vihiga/> accessed 18 August 2021

290 Kenya: Vihiga County Health Care Service Bill, 2019 [Kenya], <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/VihigaCountyHealthCareServiceBill2019.pdf> accessed 18 August 2021

291 Office of the Data Protection Commissioner, Draft Strategic Plan FY 2021-2023 <https://www.odpc.go.ke/wp-content/uploads/2021/10/ODPC-Draft-Strategic-Plan_v2.5-20211021.pdf> accessed 01 November 2021

292 ibid

293 ODPC, 'Guidance Note on Data Protection Impact Assessment' (Republic of Kenya, 2021) < https://www.odpc.go.ke/download/odpc-protection/?wpdmdl=7628&refresh=6182fde28347e1635974626> accessed 01 November 2021

294 UNICEF, 'AI For Children', <https://www.unicef.org/globalinsight/featured-projects/ai-children> accessed 18 August 2021

Open Institute

WE ARE OPEN

P.O Box 50474, Nairobi 00100, Kenya

hello@openinstitute.africa

https://openinstitute.africa