KICTANet
The Power of Communities

Public Participation

An Assessment of Recent ICT Policy Making Processes in Kenya

Grace Githaiga | Sigi Waigumo Mwanzia | Victor Kapiyo

July 2021

Contents

Executive Summary

This report assesses the extent to which the public participated in three recent ICT policy and law-making processes. These include the National Information Communications and Technology (ICT) Policy, 2019, the Computer Misuse and Cybercrimes Act, 2018, and the Data Protection Act, 2019.

While the principle of public participation is listed under Article 10 of the Constitution of Kenya, 2010 as one of the national values and principles of governance, the approach taken by state bodies in the ICT sector to facilitate public participation has been varied. Despite progress in the past decade, such as the promotion of greater stakeholder engagement, better documentation and information sharing, hosting public county meetings, and making stakeholders' inputs on publicly accessible platforms, challenges still remain.

Generally, the government is yet to put in place a holistic, multi-disciplinary, multi-stakeholder, mechanism for public participation. For example, the Public Participation Bill, 2019 which could provide the framework for effective public participation, has not yet been enacted.

Specifically, the three ICT processes were marked by cross-cutting inconsistencies in the interpretation and application of public participation. State agencies failed to: **Inform** the public with objective, baseline research to enable stakeholders to understand the problem or need to be addressed by a process, and solutions proposed; **Consult** stakeholders, and provide them with sufficient time to contribute to public calls for input, or give feedback on the consideration of stakeholder submissions; **Involve** stakeholders to contribute to the processes from the beginning, avail equal opportunities for different stakeholders to contribute to the processes, or avoid duplication of processes; and, **Collaborate** with stakeholders in decision-making to ensure consensus and balancing special interests against stakeholders' inputs, evidence and facts.

The key recommendations are as follows:

- The National Assembly should update and enact the Public Participation (No. 2) Bill, 2019. The Bill should provide principles for public participation, guidelines to the public for making oral and written submissions, prescribe standards and procedures for submissions, and set timelines for consideration and feedback.
- State agencies should give at least twenty-one (21) days notice of public participation processes, and include details of contact persons, a summary of questions being released for public consultation, a standardised format of submissions, deadlines for receipt of memoranda, and the means through which to make submissions, such as email, post or physical addresses.
- State agencies should proactively engage more 'non-traditional' stakeholders, including marginalised and minority groups such as rural communities, youth, students, children, the elderly, persons with disabilities, and the LGBTQIA+ community.
- State agencies addressing a common policy issue, should collaborate with each other and agree on a common purpose and goal with stakeholders to avoid confusion and duplication of policy and law-making processes.
- State agencies should conduct extensive and objective background, issue and evidence-based research prior to developing policies and laws and avail the research publicly to all stakeholders to provide a baseline level of evidence and facts.
- State agencies should prepare and publicly avail, in partnership with stakeholders, a guiding document(s) outlining formal procedures and mechanisms prior to the commencement of a process. This document should clearly set out the leadership, representation of the stakeholders, rules of engagement and process for contribution, inclusion and exclusion of inputs, decision-making powers and methods, accountability and redress.

1.0 Introduction

1.1 Background

ICT Policy processes in Kenya have over the past decade been secretive, highly centralised, authoritarian, and characterised by low levels of trust and the limited participation of, and contribution from non-government stakeholders. [1]

The processes have been primarily initiated, dominated and executed by the state and its agents, in its capacity as the primary duty-bearer. However, while decision-making powers may rest with the government, there is an onus placed on the government to facilitate public participation.

The principle of public participation is one of the national values and principles of governance under the Constitution of Kenya, 2010. This principle binds all state organs, state and public officers, and all persons in Kenya whenever any of them applies or interprets the Constitution, enacts, applies or interprets any laws, or makes or implements public policy decisions. While not explicitly defined in the Constitution, the term "public participation" is defined under the Public Participation Bill (No. 2 of 2019)[2] as the 'involvement and consultation of the public in the decision-making processes of the relevant state organs and public offices.'

The right to public participation is an enabler of political and socio-economic development and the realisation of numerous rights, including the right to political expression, access to information, the right to freedom of assembly and association, amongst others. Bearing this in mind, stakeholders in the ICT space should stand guided by the multistakeholder model of internet governance that has been accepted globally as an optimal standard to make policy decisions for a globally distributed network. This acceptance is reflected in declarations, resolutions, and day-to-day working practices of a growing number of international organisations and processes on ICTs and internet governance.

For example, the Tunis Agenda, which was adopted during the World Summit on the Information Society (WSIS), affirms that 'building an inclusive development-oriented Information Society will require unremitting multi-stakeholder effort from various stakeholders.[3] The WSIS+10 High Level event endorsed the multistakeholder approach stating that it was "essential" in building the information society and therefore, "should be harnessed emphasising its benefits, recognising that it has worked well in some areas; and that it should be improved, strengthened and applied in some other areas". [4]

The NETmundial conference developed a set of Internet Governance Process Principles which recognised that multi-stakeholderism and meaningful participation are core principles for an 'inclusive, effective, legitimate, and evolving Internet governance framework'.[5]

The ten Internet governance principles include:

- **Multistakeholder:** Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion.
- **Open, participative, consensus driven governance:** The development of international Internet-related public policies and Internet governance arrangements should enable the full and balanced participation of all stakeholders from around the globe, and made by consensus, to the extent possible.
- **Transparent:** Decisions made must be easy to understand, processes must be clearly documented and follow agreed procedures, and procedures must be developed and agreed upon through multistakeholder processes.
- **Accountable:** Mechanisms for independent checks and balances as well as for review and redress should exist.

Governments have primary, legal and political accountability for the protection of human rights

- **Inclusive and equitable:** Internet governance institutions and processes should be inclusive and open to all interested stakeholders. Processes, including decision making, should be bottom-up, enabling the full involvement of all stakeholders, in a way that does not disadvantage any category of stakeholder.
- **Distributed:** Internet Governance should be carried out through a distributed, decentralized and multistakeholder ecosystem.
- **Collaborative:** Internet governance should be based on and encourage collaborative and cooperative approaches that reflect the inputs and interests of stakeholders.
- **Enabling meaningful participation:** Anyone affected by an Internet governance process should be able to participate in that process. Particularly, Internet governance institutions and processes should support capacity building for newcomers, especially stakeholders from developing countries and underrepresented groups.
- **Access and low barriers:** Internet governance should promote universal, equal opportunity, affordable and high quality Internet access so it can be an effective tool for enabling human development and social inclusion. There should be no unreasonable or discriminatory barriers to entry for new users. Public access is a powerful tool for providing access to the Internet.
- **Agility:** Policies for access to Internet services should be future oriented and technology neutral, so that they are able to accommodate rapidly developing technologies and different types of use.

Likewise, the International Association for Public Participation (IAP2) in collaboration with the National Coalition for Dialogue and the Co-Intelligence Institute developed seven principles for public engagements. These include: careful planning and preparation; inclusion and demographic diversity; collaboration and shared purpose; openness and learning; transparency and trust; impact and action; and, sustained engagement and participatory culture. [6]

From the foregoing, it is apparent that both public participation and the multistakeholder model of Internet governance aims to bring together all stakeholders[7] such as businesses, civil society, governments, research institutions and non-government organizations to cooperate and participate in the dialogue, decision making and implementation of solutions to common problems or goals. [8]

Consequently, certain common attributes have emerged from the models. Some of these attributes include: open and accessible; inclusive; consensus-driven; and transparent and accountable. If consistently applied to ICT policy and law-making processes, these attributes could serve the purpose of making public policy decision-making in the ICT space more collaborative and effective, and produce workable outcomes that all stakeholders can implement. [9] Also, they can ensure that ICT policy and law-making processes continue to evolve to effectively serve the public good.

The NETmundial conference recommended the need to develop multi-stakeholder mechanisms at the national level, cognisant of the fact that a significant portion of Internet governance issues should be tackled at the national level.[10] These mechanisms could also serve as a link between local discussions and regional and global processes, thus enabling fluent coordination and dialogue across the different levels.

This paper assesses the extent to which recent ICT policy and law-making processes in Kenya such as the development of the National ICT Policy 2019; the Computer Misuse and Cybercrimes Act, 2018; and the Data Protection Act and Data Protection Policy 2019 facilitated public participation and complied with the multistakeholder approach.

This assessment is based on the Global Partners Digital (GPD) Framework for Multi Stakeholder Cyber Policy Development and assessed the extent to which each of the national policy and law-making processes was: open and accessible; inclusive; consensus-driven; and transparent and accountable.[11]

1.2 Methodology

In conducting the assessment, the research team documented the historical development of the three processes from their commencement to completion, using publicly available and privately-sourced information.

This historical development was informed by qualitative material, including reports of previous studies, print and digital media reports, academic works, government documents, and other literature.

This desk research was supplemented by key informant interviews conducted **between September and October 2020** with purposely selected respondents drawn from various multi-stakeholder groups, who participated in the three processes.

The processes were then assessed and benchmarked against the Global Partners Digital (GPD) Framework for Multistakeholder Cyber Policy Development. [12]

The team utilised the GPD diagnostic toolkit, which contains a specific set of indicators, sub-indicators and guiding questions to assess the extent to which each process was: open and accessible; inclusive; consensus-driven; and transparent and accountable.

Open and accessible

Consensus-driven

Inclusive

Transparent and accountable.

The findings from this assessment inform the recommendations in the report.

There were limitations to the study that impacted our ability to cover the topic with more depth and complexity.

These included poor reporting and documentation by state actors, limited data and reliable or conflicting information on the topic, and potential interviewer bias during the informant interviews.

2.0 The Case Studies

This section reviews three ICT policy and legislative processes, namely the development of:

1. **The National Information Communications and Technology (ICT) Policy, 2019;**
2. **The Computer Misuse and Cybercrimes Act (2018); and,**
3. **The Data Protection Act, 2019.**

2.1 The National Information Communications and Technology (ICT) Policy, 2019

Prior to the enactment of the 2006 ICT Policy, the ICT sector in the country was regulated by the Telecommunications and Postal Sector Policy Guidelines (1997), [13] **the Kenya Information and Communications Act (1998), and the Telecommunications and Postal Sector Policy Statement (2001).** [14]

Through these instruments, the government committed to 'continuously review policies in the (ICT) sector to ensure that they remained relevant to the development of the communications industry.' [15]

The 2001 policy was the result of 'extensive consultation with stakeholders in the telecommunications and postal sector and the public.' [16] *Following this, in March 2006, the first*[17] *national ICT Policy,*[18] *was adopted following an extensive multi-stakeholder consultation process, of which one of the outcomes was the creation of KICTAnet.*[19] *The mission of the policy was to improve the livelihoods of Kenyans by ensuring the availability of accessible, efficient, reliable and affordable ICT services.*[20] *Notably, it was guided by four principles, namely: 'infrastructure development, human resource development, stakeholder participation and appropriate policy and regulatory framework.'* [21]

The policy remained in force until 2019, when the 2019 National ICT Policy was adopted. However, between 2006 and 2019, the government developed various policy documents including the National ICT Masterplan (2014-2017), [22] the National Broadband Strategy (2013), [23] and the National Cyber Security Strategy (2014). [24] The development of the National ICT Masterplan was spearheaded by a 12-member taskforce, while the National Broadband Strategy was developed by a National Steering Committee, which bodies engaged with stakeholders on the draft documents prior to final approval.

The National ICT Masterplan (2014-2017) recognised that the 2006 ICT policy had not been updated despite global technological developments and national ICT sector changes in Kenya. The Masterplan urged for its revision to take into account the changes which emerged since 2006, including Vision 2030; the Constitution; new sectoral strategies; and other realities.[25] In 2015, a draft ICT policy was developed by the Ministry of ICT and was expected to be finalised 'as soon as possible.' [26] However, the draft was recalled for re-drafting after 'extensive consultations' and the need for 'further input aimed at providing a more inclusive document incorporating new and emerging issues within the ICT sector.' [27]

In January 2016, KICTAnet presented the newly appointed Cabinet Secretary for ICT, Joe Mucheru with an ICT wishlist with various policy priorities for his first 100 days in office.[28] On 17 March 2016, the Cabinet Secretary for ICT, announced the review process of the draft ICT policy, and invited stakeholders to submit their views on the draft policy.[29] The Cabinet

Secretary stated that the review of the 2015 draft was necessary as "it was felt that it required further input aimed at providing a more inclusive document incorporating new and emerging issues within the ICT sector."[30] He also indicated that the policy review "would take a multi-sectoral approach, with input from all stakeholders."[31] The process was expected to be completed by June 2016.[32]

Subsequently, the review of the draft ICT policy commenced in earnest with a multi-stakeholder approach spearheaded by the National Communications Secretariat (NCS) and the Ministry of ICT, facilitated through three working groups comprising stakeholders drawn from the ICT sector, and the general public. The three working groups included: Infrastructure; new and emerging issues; and Devices, applications, and content, which were chaired by different stakeholders groups including KICTAnet and KEPSA.[33] The working groups met regularly and developed reports which were then presented to the NCS for consolidation into a zero draft.'[34]

The draft ICT Policy (2016)[35] was eventually availed to the public for comments on 8 June 2016 and the public participation process culminated with a validation meeting on 6 July 2016.[36] During this meeting at Laico hotel in Nairobi, the working groups met in break-away groups in separate rooms and thereafter presented their final reports to the NCS for collation.[37]

On 28 October 2016, it was reported that the draft ICT policy had been submitted to the ICT Ministry 'for review before its presentation to the Cabinet for approval.'[38] However, on 31 January 2017, the Ministry of ICT indicated that the review process was still ongoing, and that 'students and institutions would be consulted to ensure that their views were incorporated.'[39] The processes stalled at this stage and it was only on 14 October 2019, that the document was reported to be in the final revision stages before being presented to the Cabinet for approval.'[40]

Following the three-year hiatus, which can be referred to as the 'post-Laico black hole', the National ICT Policy received Cabinet approval on 30 December 2019.[41] This policy states that it was 'formulated after broad-based public consultations in a number of iterations.'[42] However, it significantly varies from the 2016 draft shared with the public[43] and was not subjected to a public participation process prior to its enactment.

Moreover, the announcement of its adoption was made through a post on the Ministry of ICT's Twitter handle on 31 December 2019.[44] On 7 August 2020, the National ICT Policy Guidelines (2020) were gazetted.[45]

2.2 The Computer Misuse and Cybercrimes Act, 2018

The Kenya Information and Communications Act, 1998 (KICA) initially provided for ICTs and cybercrimes. However, the law was not sufficient and the country lacked a comprehensive cybercrimes law. In 2013, KICA was amended by the Kenya Information and Communication Amendment Act (2013) which came into effect on 2 January 2014.[46] The amendments resulted in, among others, the establishment of the National Cyber Incident Response Team;[47] the restructuring and renaming of the Communications Commission of Kenya (CCK) to the Communications Authority (CA), with a wider mandate including prosecutorial powers; and the introduction of SIM card regulations.[48]

In 2014, the Office of the Director of Public Prosecutions (ODPP) developed a draft Cybercrime and Computer-related Crimes Bill (2014) to provide a comprehensive legislative framework for cybercrime.[49] The Bill was geared towards equipping the ODPP and other 'law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime'[50] as evidenced by its objectives. This draft was subsequently withdrawn following concerns of the role of the ODPP as the national prosecuting authority in Kenya, leading the development of a cybercrime law.

During the same year, the ICT Ministry published the 'National Cyber Security Strategy' (2014), which recognised cybersecurity as a national priority.[51] Kenya's National ICT Masterplan (2014-2017) called for the development, implementation and institutionalisation of a cyber security management framework; implementation of the Cyber Security Master Plan and the development of a cyber security policy.'[52] In December 2015, the CA released the draft Kenya Information Communications (Cyber-Security) Regulations 2016 and the draft Kenya Information Communications (Electronic Transactions) Regulations 2016 for public comments.[53] The CA held public consultations on both regulations on 18 April 2016, with a deadline of 21 April 2016 for written memoranda.[54]

A draft Critical Infrastructure Protection Bill (2015) was also published.[55] However, none of these were enacted. During this entire period, stakeholders at the national, regional and international levels ramped up lobbying and advocacy efforts for a comprehensive cyber security framework to address cybersecurity challenges, embrace best practice and adopt proper cybersecurity standards.[56]

The year 2016 saw further developments in the policy

and legislative arena with the development of the draft National ICT Policy (2016), draft ICT Capacity Bill (2016), draft Computer and Cybercrimes Bill (2016), and the draft Cybersecurity and Protection Bill (2016). These developments had significant implications on the trajectory of the cybercrimes legislative agenda. Notably, the draft National ICT Policy 2016 called for the development of 'appropriate legal and regulatory frameworks' with an 'extra territorial' outlook and approach towards cybercrimes.'[57] Further, it identified cyber security as a 'key objective of national security'.

In 2016, it emerged that there were two identical processes to enact cybersecurity and cybercrimes legislation. On the one hand, the Senate was developing the draft Cybersecurity and Protection Bill (2016), while on the other, the Ministry of ICT was leading the development of the draft Computer and Cybercrimes Bill (2016).

The Cyber Security and Protection Bill 2016 was first tabled in the Senate on 5 July 2016, by Mutahi Kagwe, the then Chairperson of the Committee on Information and Technology.[58] The Bill sought to provide for among others, 'increased security in cyberspace' and for 'the prohibition of certain acts in the use of computers.' The Committee invited the public to participate in public hearings on 19 October 2016, and written memoranda on the Bill were expected to be submitted the same day.[59] However, the Bill was subsequently withdrawn,[60] paving way for the development of the Computer and Cybercrimes Bill (2016).

The ICT Ministry continued receiving input[61] on the Computer and Cybercrimes Bill (2016)[62] from various national, regional and international stakeholders between 2016 and 2017. The draft Bill had been generated by an Inter-Agency Technical committee which was chaired by the Kenya Law Review Commission, and consisted of state and non-state actors.[63]

The Bill was approved by Cabinet in May 2017 and forwarded to the Attorney General.[64] On 13 June 2017,[65] the bill was tabled in the National Assembly as the Computer and Cybercrimes Bill, 2017 and underwent the first reading on 10 October 2017. It was then referred to the Departmental Committee on Communication Information and Innovation for consideration, which submitted their report to the House for the second reading on 11 March 2018.

Prior to this, the Committee issued a call for comments from the public on 6 February 2018 that were to be received by 13 February 2018. The Committee only received 13 memoranda[66] from various stakeholders,[67] who were formally invited to separate meetings with the Committee on various dates in February 2018.[68]

The Bill underwent the second reading between 22 – 29 March 2018 and again on 2 April 2018. It was subsequently referred to the Committee of the whole House, and considered on 26 April 2018, where it was read the 3rd time and passed.[69] Notably, there were significant amendments to the Bill made during debates on the floor of the house.[70]

The Bill was then assented to by the President on 16 May 2018 and came into effect on 30 May 2018, as the Computer Misuse and Cybercrimes Act, 2018.

> ***"This law also touches on the security sector ... but the Bill belongs to the Ministry of Information, Communications and Technology."***[71]
>
> ***"There are people who earn their living through extortion by using this technology. They harass your family and run such stories for weeks. They have over one or two million followers. They create fake videos and ultimately you pay them to stop and that is how they earn their living… There are people who go to an accident or terrorist site and take pictures which are not good for the family and children and put this in WhatsApp groups. If you are (an) administrator of a WhatsApp group and you are watching me, by the time this Bill is signed into law, there will be very few administrators of WhatsApp groups."***[72]

Following its assent, the Bloggers Association of Kenya (BAKE) in May 2018, filed a petition challenging the constitutionality of the Act and 26 of its provisions.[73] They also argued that 14 provisions introduced by individual members during [the] committee of the whole' were not subjected to public participation.[74]

The High Court initially suspended the application of the 26 provisions of the Act, but in February 2020 found the entire Act to be constitutional, which decision is being challenged before the Court of Appeal.[75] However, in October 2020, the High Court in a separate case, nullified the Computer Misuse and Cybercrimes Act, 2018, on grounds that the Senate's input had not been sought.[76] This order was suspended for a period of 9 months, until June 2021.[77]

2.3 The Data Protection Act, 2019

Efforts by various stakeholders to implement a comprehensive privacy and data protection framework commenced well before the right was enshrined under Article 31 of the Constitution of Kenya, 2010.

The Data Protection Bill (2009)[78] was published by the Ministry of Information and Communications in June 2009, and subsequently received and considered by the Commission for the Implementation of the Constitution (CIC) between July 2011 and September 2012.[79]

The CIC audited and subsequently aligned the Bill with the Constitution and Kenya's international obligations, relying on stakeholder input. The CIC held various stakeholder consultations with non-state actors prior to September 2012, and with state actors including the Attorney General, the Kenya Law Reform Commission, the Ministry of Information and Communications, and the Commission on Administrative Justice between 1 - 2 October 2012.[80]

In 2013, the the Attorney General, revised and published the Data Protection Bill, 2013,[81] which was expected to be tabled before the National Assembly in May 2014, by the Ministry of ICT.[82] However, the Bill was not tabled before the National Assembly as expected.[83] Between 2011 and 2016, legislation such as the National Payment System Act (2011),[84] the Consumer Protection Act (2012), [85] the Kenya Information and Communications Act (KICA) (2012),[86] new regulations under KICA, such as the Consumer Protection Regulations (2010)[87] and the Registration of SIM-Cards Regulations (2015), [88] and the Access to Information Act (ATI Act) (2016)[89] were adopted. However, these laws did not provide an adequate legal framework for the protection of the right to privacy.

Despite ongoing conversations, the Data Protection Bill was not enacted due to the lack of political will at the time. Therefore, key stakeholders, especially civil society, directed their energy and efforts toward the adoption of the Access to Information Act, 2016,[90] and incorporated provisions on privacy and data protection in the law.[91] The Commission on Administrative Justice (CAJ) was subsequently granted a broad mandate in the Act to oversee the implementation of the right to access information and data protection under the Constitution.[92] Despite these dual responsibilities, the CAJ has over the years focused more on its access to information, rather than data protection mandate.

Between 2013 and 2018, there were no further developments with respect to the Data Protection Bill, 2013. Subsequently, on 30 May 2018, Gideon Moi, Chairperson of the Senate Committee on Information, Communication and Technology tabled the Data Protection Bill, 2018 (Senate Bill). [93] The Senate Bill, primarily intended to 'protect personal data collected, used or stored by both private and public entities.' [94] During the same month, the Cabinet Secretary for ICT, through Gazette Notice No. 4367 dated 11 May 2018, constituted the 'Taskforce on the Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya'.[95] The Taskforce was mandated over a three-month period, to primarily develop a policy, legislative and institutional framework for privacy and data protection in Kenya.

As the Taskforce commenced its work, the Senate Bill underwent the first reading on 3 July 2018. In August 2018, the ICT Ministry published the Privacy and Data Protection Policy 2018 - Kenya[96] and the Data Protection Bill 2018 - Kenya (Taskforce Bill)[97] as drafted by the Taskforce.[98] The main objective of the Policy was to inform the development of a data protection framework, facilitate statutory and regulatory compliance and enhance the effective implementation of the proposed data protection law in Kenya. The Taskforce Bill was expected to 'govern the enforcement of Article 31 of the Constitution of Kenya on the right to privacy.

> ***CS Joe Mucheru excerpt:*** ***"The Taskforce that is working on data privacy (has) almost completed their stakeholder engagement ...(and are) about to produce a draft that will help in terms of the data storage that… you will see happening as we expand… Data protection is key...ownership of… own… personal data is important."***[99]

The public was given five (5) working days to submit comments on the Taskforce Bill from 13 September 2018 to 19 September 2018,[100] but this was later extended to 2 October 2018 for written memoranda, and 3 October 2018 for public hearings.

In addition, the Taskforce indicated that it would accept comments past the deadline, as well as grant audience to stakeholders who made formal requests for hearing.[101] The ICT Ministry intended to submit the Data Protection Policy and Bill to the National Assembly on 31 October 2018.

Meanwhile, the Senate Bill underwent the second reading on 6 - 7 November 2018. From November

2018 and May 2019, there was a stalemate between the ICT Cabinet Secretary and Senate's ICT Committee over 'contentious clauses' and the simultaneous development of the Taskforce Bill.[102] On 8 May 2019, following deliberations between the Senate ICT Committee and the Cabinet Secretary for ICT, consensus was reached to incorporate proposals advanced by the ICT Ministry into the Senate Bill, including providing for an independent data protection authority.[103]

This Bill was then expected to be presented for the third reading before the Committee of the Whole on 14 May 2019. Despite these consultations, it later emerged that the Ministry of ICT had, by 18 April 2019, sought and obtained Cabinet approval of the Data Protection Policy and Bill, 2018.[104]

> ***CS Joe Mucheru excerpt:*** *"I am being informed that the AG had directed that the approved Bill by the Cabinet needs the input of the National Assembly. I know this is contrary to what we agreed and I seek more time to go and consult."*[105]

The Data Protection Bill, 2019 (National Assembly Bill, 2019)[106] was published on 21 June 2019, and tabled in the National Assembly for the first reading on 4 July 2019. The Senate got wind of this development on 19 June 2019 and cut short its session after receiving the information.[107]

The Cabinet Secretary for ICT maintained that the Cabinet had approved the Bill at the National Assembly and insisted that the process at the National Assembly proceed, as directed by the Attorney General Kihara Kariuki.[108] The Senate Bill is still pending consideration by the Committee of the Whole House to date, and has not progressed or been withdrawn.[109]

Based on the foregoing, the process at the Senate was bypassed by the National Assembly, rendering the months-long deliberation process of the Senate Bill moot. The Senate opposed[110] the move by the Executive to prioritise the Bill at the National Assembly, which undermined the Senate's law-making authority as it ostensibly implied that data protection did not affect county governments in Kenya.

Nonetheless, the Bill at the National Assembly was referred to the Departmental Committee on Communication, Information and Innovation and underwent the second reading between 29 - 30 October 2019 and 6 November 2019.[111]

The Committee invited the public to give input on the Bill between 11 July 2019 to 16 July 2019 through public notices in local dailies (Daily Nation and the Standard newspapers).[112] Following this, the Committee hosted 15 meetings with the stakeholders and considered a total of 16 memoranda from members of the public and institutional stakeholders in the ICT sector.[113]

The Bill underwent the third reading and was passed by the National Assembly on 7 November 2019. It then received presidential assent on 8 November 2019 and came into effect on 25 November 2019 as the Data Protection Act (No. 24 of 2019). [114]

In November 2020, Immaculate Kassait was appointed as the first Data Protection Commissioner, following her nomination by the President and approval by the National Assembly.[115] Kassait will serve as the Commissioner for a 6 -year period, as set out in the Data Protection Act (2019).[116]

Meanwhile, a constitutional petition challenging the constitutionality of the Act was filed in November 2019 by a public interest litigator, Okiya Omtatah, and remains pending determination before the High Court.[117]

3.0 Results

This section provides a comparative assessment of the three ICT processes highlighted above using the 'Diagnostics Tool for Inclusive Cyber-Policy Making'. It reviews the extent to which each process was 'open and accessible', 'diverse', 'collaborative', 'consensus-driven', 'evidence-based', and 'transparent and accountable'. Further, it highlights instances where strong guarantees of inclusive ICT policy were observed, and the specific challenges which constrained the processes.

3.1 Positive Aspects

3.1.1 Open and Accessible

This indicator assessed the extent to which participation in the processes were open and accessible to stakeholders. This included the presence of active measures to enable participation such as notice given well in advance and distributed via relevant channels, and the efforts taken to address obstacles or barriers that may have prevented or discouraged participation, including financial, geographical and language barriers.

Highest score: Data Protection Process

Generally, this process was the most open and accessible across all stages for a number of reasons. There was heightened public interest in data protection and privacy issues, sparked by ongoing national events, such the introduction of Huduma Namba, and the global trend towards the adoption of national data protection laws following the adoption of the GDPR in the European Union.

In addition, political will was high at the time as evidenced by the parallel legislative processes in both houses of Parliament. Thirdly, the parliamentary and the Taskforce processes provided significant opportunities for various stakeholders, including CSOs and academia, to invest, engage and contribute to the development of the laws. Further, CSOs who had engaged in the development of the ATI Act, 2016 built on this momentum and channelled their energies towards the development of a comprehensive, stand-alone privacy protection framework.

The public interest was coupled with goodwill from the Data Protection Taskforce and the parallel Parliamentary processes, which provided several opportunities for interested stakeholders to contribute to the development of the data protection law. For example, despite notable time challenges affecting all stages of the process, the Data Protection Taskforce extended the time from an initial 5 working days to 14 working days (13 September - 2 October 2018) for public comments with an additional day on 3 October 2018, to receive comments.

Building on this, the National Assembly ICT Committee shattered the 'Nairobi-centric' nature of ICT policy process, by hosting additional public forums in Kakamega, Mombasa, Kilifi, Kisumu, Kericho, and Nakuru counties to ensure geographic balance. In comparison to the cybercrimes and ICT policy processes, the engagement of county-based stakeholders elevated and set a new standard of openness and accessibility for subsequent ICT policy-making processes.

The Taskforce, Senate and the National ICT Committees provided stakeholders with a variety of physical and virtual platforms to participate and contribute to the data protection processes. The bodies circulated public notices calling for stakeholder input and notifying them of public meetings

in newspapers of national circulation. Also, stakeholders could remotely submit their written memoranda via email or through the post, or present them orally in person during public meetings and targeted meetings with select stakeholders and virtually, via video conferencing platforms, such as Zoom. Likewise, stakeholders engaged in discussions on the laws in various forums and collectively worked to develop their submissions to the law-making bodies.

Further, the availability of stakeholders' written submissions and memoranda on the CA's website, as well as in the National Assembly's Committee report, showed the stakeholders who participated, thus demonstrating the level of openness and accessibility.

What worked well across the other two processes?

In comparison to the data protection process, the ICT Policy and the cybercrimes processes had a few successes under this indicator. The ICT Ministry held public consultations at the Intercontinental Hotel (cybercrimes) and the Laico Hotel (ICT Policy), both of which provided physical access for persons with physical disabilities.

Moreover, the National Communications Secretariat put out calls for public participation for the draft ICT Policy for a month from 8 June 2016 till 6 July 2016. This period is in line with the proposed 21-day period stipulated in the draft Public Participation Bill, 2019 and, at the very least, presented stakeholders with sufficient time to respond and give input to the development of the draft ICT Policy, 2016.

3.1.2 Diverse

This indicator assesses the degree to which the processes were diverse and the extent to which the different views and interests of the stakeholders were allowed, heard and considered, the opportunity given to stakeholders to contribute, and the level of consideration given to their inputs.

Highest score: Data Protection Process

This process was the most diverse, with a wide range of views and interests being presented, and the highest level of consideration given to the stakeholder inputs. There was input, buy-in and support from diverse stakeholders.

These included individuals (teachers, lawyers, public interest litigants and activists); the government (MoICT, TSC, KNCHR and CAJ); foreign government (U.S. Department of Commerce's International Trade Administration and the Council of Europe's Data Protection Unit); tech companies (Safaricom, Airtel, Amazon Web Services, Facebook, GSMA, IBM, Google Kenya, Microsoft, Uber, Mozilla, Multichoice Kenya, and Atlancis Technologies Limited); insurance companies (AIG Kenya); law firms (Bowmans, Baraza and Kijirah Advocates and Chebet and Munyaka Advocates); financial services (KCB Kenya, Mastercard Kenya, M-Kopa Solar, FSD Kenya, Branch International Limited and Tala); private sector associations (KEPSA, DLAK, KMA, KENIC, TESPOK, ICTAK, and ISACA); academia (CIPIT and Research ICT Africa); the media (Media Council of Kenya); civil society (Amnesty International Kenya, ARTICLE 19 Eastern Africa, Bunge la Wazalendo, KICTANet, Privacy International, NCHRD-K, and Lawyers Hub); were well-represented during the 2018 - 2019 processes, in varying degrees.

The concerns relating to the rights of children, the rights of PWDs, and whistleblowers were raised by various stakeholders to the NA Committee during public forums held in Mombasa, Kilifi, Kericho, Kakamega, Kisumu, Nairobi, and Nakuru counties.[118] Conversely, the NA Committee report does not contain information about specific concerns relating to the LGBTQIA+ community, the youth and refugees. However, it is likely that these groups' opinions were collated and incorporated into the submissions of more dominant groups, which actively raised awareness on data protection in Kenya.

Among some stakeholders groups, three organisations stood out, including the Kenya ICT Action Network, ARTICLE 19 Eastern Africa and the Centre for Intellectual Property and Information Technology (CIPIT) who reached out to their partners and the general public, using

a variety of online and offline tools, reported back and fed material and updates to the wider community, but in varying degrees. The organisations used focus group discussions, hosted widely inclusive dialogue fora and targeted diverse groups, including journalists, data protection experts, lawyers, academia, data scientists, and bloggers.

KICTAnet's submission reflected the views and comments of diverse stakeholders following discussions on its mailing list. CIPIT partnered with the National Coalition of Human Rights Defenders – Kenya, and Privacy International collated feedback from a large group of HRDs in Kenya. ARTICLE 19 EA also collated responses at the county-level, in Mombasa, Nakuru and Nairobi, in conjunction with CIPIT, KICTAnet and technology hubs in Kisumu, Mombasa and Nairobi Counties, which informed its submission.

These tools diversified the range of views and interests within the participating stakeholder group, encouraged dialogue and discussion on the different iterations of the Data Protection Bill, and helped to enrich and consolidate perspectives that informed their submissions on the Bill. Notably, the discussions resulted in a high level of convergence around issues such as the independence of the data commissioner, the rights of data subjects and principles of data protection. There was divergence between private and public stakeholders on the issues of data localisation and automated data processing.[119]

What worked well across the other two processes?

The ICT Policy process was hailed for its consensus-based approach in the development of the initial 2016 draft which pointed to the existence of 'high buy-in' from stakeholders.[120] Similarly, the National Assembly's ICT Committee, in its report on the Computer and Cybercrimes Bill, 2017, considered the stakeholder inputs it received.

In its report, the NA ICT Committee analysed the written stakeholder inputs explicitly referencing them, and summarised the submissions during the public county meetings on the various clauses of the Bill and contains the Committee's recommendations. As one interviewee noted, this report 'goes argument by argument which was very helpful'[121] and offers insights into good reporting practices which can be emulated in similar processes. Moreover, the availability of the Parliamentary Hansard online provides critical insights about the debates on the Computer and Cybercrimes Bill, 2017, at the floor of the House.

3.1.3 Collaborative and Consensus Driven

This indicator assessed the extent to which the processes were consensus-driven, and whether the participants acted with common purpose, in a collaborative manner and, as far as is possible, took decisions by general agreement. The willingness of stakeholders to cede ground and compromise, and the treatment of dissenting voices was also considered. This section also assessed the extent of collaboration, commitment to the common purpose and whether the participants built trust and strong relationships.

Highest score: ICT Policy Process

The ICT Policy process was the most collaborative and consensus-driven. This process was stakeholder-driven and had a common purpose to review and develop the policy. This drive was based on the pressing need and demand from ICT stakeholders to the MoICT to update the 2006 Policy, which hadn't been 'updated … for close to eight years despite global technological developments and national ICT sector changes in Kenya.'[122]

The process was guided by a deliberate bottom-up and collaborative approach from the commencement of the process to the development of the draft 2016 ICT Policy. Following the ICT Ministry's announcement of the process, the NCS reached out to various stakeholders to volunteer, join, participate and lead the collection of views and the drafting of sections of the draft 2016 ICT Policy. The creation of three multi-stakeholder working groups on infrastructure, new and emerging issues, and devices, applications, and content demonstrated the government's interest to hear the perspectives of different stakeholders, whose contributions ultimately fed into the draft 2016 ICT Policy.

The initial drafting process was led by, and composed of, diverse stakeholders who met regularly and developed the draft sections of the policy from scratch, which were then consolidated into the draft 2016 ICT Policy. The Working Groups had 'fairly flexible terms of reference which did not restrict the WG chairs

from adding other topical issues which they believed were central to the Working Groups' mandate.'[123]

The stakeholders worked well together and had various opportunities to build new, and strengthen existing relationships which have continued over time. This occurred during the working group meetings, the public participation meeting at Laico Hotel, and through virtual forums, such as the KICTAnet mailing list where stakeholders constructively engaged each other and made decisions by consensus. The process demonstrated that there was a general commitment to collaborate and ensure that the ICT Policy, 2006 was updated.

Generally, this process leading to the draft ICT Policy 2016 speaks to the existence of trust between the ICT Ministry, the NCS and stakeholders in the ICT sector. The stakeholders' submissions of a draft ICT Policy 2016, rather than proposals on what could be included in the draft Policy, is a testament of the high level of trust, collaboration and consensus.

What worked well across the other two processes?

In the cybercrimes and data protection processes, strong collaborative relationships were formed between stakeholders. Some of these already existed, while others were created organically during the processes. Others were born out of the need to present a unified 'multi-stakeholder' voice, capable of pushing back against problematic provisions in the draft Bills.[124] Notably, collaboration of stakeholders with the ICT Committees of both the Senate and the National Assembly was strengthened as a result of the various opportunities for stakeholders to make presentations before them.

During the cybercrimes process, stakeholders 'managed to shatter the extreme content-based nature of the cybercrimes Bill' despite their fear of 'pushing back too hard and subsequently being excluded'.[125] Some of the areas where collective stakeholder push-back was successful included the repeal of content-based provisions on hate speech and pornography, and the establishment of a National Computer and Cybercrimes Co-ordination Committee, which was not present in the Computer and Cybercrimes Bill, 2017.[126] During the data protection process, decision-making at the data protection Task Force level was consensus-based including on 'contentious issues'.[127]

Across both processes, collaboration was strengthened through in-person meetings, representation in public hearings, discussions on online mailing lists such as the KICTAnet mailing list, joint submissions of memoranda, press statements, engagements on social media, submissions on Kenya to the Universal Periodic Review process and the ACHPR, and through strategic public interest litigation.[128]

To a large extent, collaboration in the ICT policy and legislative sphere has become an established norm in Kenya. This collaboration of stakeholders has since extended to other ICT policy processes, including advocacy on the Huduma Namba. Further, some of these relationships morphed into regional coalitions. One such coalition is the African Internet Rights Alliance (AIRA) which is a coalition of nine regional organisations, five of which operate in Kenya and were instrumental in at least two of the three policy processes.[129]

3.1.4 Evidence Based

This indicator assessed the balance of expertise and research in the process, including the existence of relevant and balanced expertise, and baseline research to support the processes. This indicator also assessed the level of agreement on the interpretation and use of evidence and facts, and the extent to which decisions were made based on the available facts and evidence.

Highest score: Data Protection Process

Generally, the data protection process was more expertise-driven and stakeholders investigated evidence and facts before and during the Parliamentary processes, as compared to the cybercrimes and the ICT Policy process.

Based on the quality and diversity of submissions, it is evident that stakeholders were knowledgeable on data protection. The knowledge and expertise of stakeholder groups varied. Instructively, some

https://www.kictanet.or.ke/

stakeholders were involved in the process since 2007, whereas others became immersed in the data protection conversation during the NA Committee's public hearings in July 2019. The Taskforce membership was diverse and drawn from individuals with relevant expertise on privacy and data protection, including research, policy, infrastructure, rights and technology.

The Taskforce conducted background research on data protection which supported the process and provided the members with a baseline level of knowledge. The Taskforce also took steps to bridge any capacity and knowledge gaps, by 'holding consultative sessions with leading data protection experts'[130] from different countries with data protection legislation and established data protection oversight mechanisms.

These included the South African and Ghanaian Data Commissioners, the Council of Europe's Data Protection Unit, amongst others.[131] One interviewee noted that 'the meetings were for both capacity building (for Taskforce members who heard and learnt from the perspectives of various experts) and exploring and understanding of contentious issues such as the debate on cloud-based data storage and data localisation.'[132]

Additionally, space and time was allocated to discussing and interpreting opinions and evidence, especially at the Taskforce and National Assembly Committee levels, and amongst stakeholders in numerous online and offline meetings held between 2018 - 2019. Stakeholders' also organised meetings and other fora for training and capacity-building purposes and to provide a space for stakeholders to assess the evidence and discuss pertinent data protection challenges and solutions.

Generally, Kenya's Data Protection Act 2019 reflects the issues raised by stakeholders based on the evidence and facts available. For example, a number of principles and rights in Kenya's DPA, 2019 are based on the EU GDPR, which stakeholders promoted as the best standard on data protection.

What worked well across the other two processes?

During the draft ICT Policy 2016 process, the multi-sectoral Working Groups were composed of individuals with a wide range of expertise and knowledge on ICT issues in Kenya. Owing to the fact that the process was community-driven, there was sufficient and extensive time provided to ensure that stakeholders contributed to the process.

During the cybercrimes process, various experts were provided with an opportunity to make submissions to the NA ICT Committee during the public participation window. Generally, the constitution of specialised expert-led mechanisms such as the Inter-agency Technical Committee (cybercrimes) and the various working groups (ICT Policy) to spearhead the processes was also a positive step.

3.1.5 Transparent & Accountable

This indicator assessed whether there were clearly defined and transparent procedures and mechanisms and the extent of compliance with the procedures.

This section also assessed other aspects, including the disclosure of stakeholder interests and affiliations; existence of clear systems of records management and documentation; clarity and adequacy of the lines of accountability internally between the leadership and group, as well as externally between stakeholders and their wider communities.

Highest score: Data Protection Process

Generally, the Data Protection processes scored the highest score under this indicator, and it was relatively easy to identify a stakeholder's interest and grouping they represented, given clear-cut delineations in the Kenyan jurisdiction. These claims had either been affirmed by virtue of registration requirements (e.g., for NGOs, telco operators etc.,) through previous engagements, or through established practice and were accepted by other stakeholders as legitimate.

However, it remains unclear whether entities operated 'in the shadows' without disclosing their interests, although there are claims that 'big tech (multinational) companies exerted some powers without openly disclosing this at the ICT Ministry level.'[133]

At the National Assembly Committee level, most stakeholder contributions were well captured, analysed and published. Likewise, at the Taskforce level, the general

environment and ethos with which the process was conducted welcomed different stakeholders to contribute.[134] The submissions by the stakeholders during both processes remain publicly available. The CA continues to host stakeholders' written submissions on its website[135] while the stakeholders' written submissions on the Data Protection Bill and the Committee's recommendations are included in the NA Committee's report on its consideration of the Data Protection Bill, which is available on Parliament's website.[136]

Further, all state agencies were guided by pre-existing and clearly defined mechanisms and procedures which steered the data protection Bill and policy processes. These are located either under the Constitution of Kenya, standing orders, legislative frameworks, ministerial powers, amongst others. Thirdly, stakeholders at the non-governmental level, did not object to each other's points and interests, but rather 'contested the draft documents'[137] themselves.

What worked well across the other two processes?

The ICT policy and the cybercrimes process were both steered by some pre-established accountability procedures and mechanisms, which are located in the Constitution of Kenya, standing orders, legislative frameworks, ministerial powers, amongst others. However, adherence by government agencies to these procedures and mechanisms varied between the two processes.

3.2 Challenges and Constraints

3.2.1. Limited Openness and Accessibility

This section identifies the challenges to stakeholder participation in the processes due to limited openness and accessibility. This included the lack of active measures to enable participation such as the failure to issue and publicly avail timely notices and documents, and the barriers that prevented or discouraged participation, including financial, geographical and language barriers.

Likewise, it assessed the extent to which the processes complied with the Access to Information Act, 2016. The Act provides that public entities before 'initiating any project, or formulating any policy, scheme, programme or law', to 'facilitate access to information,' 'publish relevant facts during the policy formulation process,' and 'communicate with the public and affected persons about facts which promote the principles of natural justice and democratic principles,' including the 'procedure followed in the decision making process.'[138]

Additionally, public entities[139] are required to disseminate information with the following considerations in mind: 'the need to reach persons with disabilities, the cost, local language, the most effective method of communication in that local area, and the information shall be easily accessible and available free or at cost taking into account the medium used.'[140] Finally, the information should be 'made available on the Internet, provided that the materials are held by the authority in electronic form.'[141]

Lowest Score: Cybercrimes Process

Generally, the cybercrimes process was the least open and accessible. During the Inter-agency Technical Committee stage, restrictions to stakeholder participation were enforced but were not explained. The Technical Committee did not permit participation by *any* interested stakeholder, failed to seek input from the public on its affairs and deliberations, and did not disclose the procedure followed in the decision-making process.

As one respondent noted, stakeholders who wanted to participate had to 'demonstrate expertise', and even so, not all who expressed interest were permitted to participate. Also, many stakeholders who possessed relevant expertise, were not aware that such a process was ongoing, given the secrecy that clouded the process. Further, the Technical Committee failed to facilitate access to information and communicate with the public and affected persons about facts, with an impact on the principles of natural justice and democratic principles.

For example, the Technical Committee was composed of pre-selected members who were largely drawn from government agencies, with only one known civil society representative. Also, one respondent revealed that they had a short time to digest the contents and contribute to the draft Bill before it moved across the other stages of the process.

At the Parliamentary level, the process was marked by radically divergent and unrealistic notice periods. For example, the Senate ICT Committee invited the public to participate in public hearings on 19 October 2016 from 11 am - 12:30 pm, and written memoranda were expected the same day. At the National Assembly, the ICT Committee granted the public five working days - from 6 February - 13 February 2018 to submit their written memoranda.

One respondent stated that the short notice period by the Senate affected the stakeholders who contributed to the Senate call for oral comments. The respondent stated, "we were the only people (about three to four individuals) who went to Senate that morning because it was so abrupt…while the Bill may have been published earlier, you cannot call people to engage in the public participation process on a Friday and expect people to show up, ready on a Monday…not everyone could make it, especially people who had to travel… you had to really rush, drop everything."[142]

This illustrates the impact of short timelines, financial costs and geographical barriers that prohibited stakeholders' ability to participate in the process. In effect, these challenges limited the effective participation of all stakeholders in the formulation stage of the process.

What did not work well across the other two processes?

Poor Notification and Dissemination of Information on the Processes

Under clause 10 of the Public Participation Bill No. 2 of 2019, state organs and public officers are required to ensure that a public participation forum is 'fully publicized to enable the attendance and participation of a wide section of the public, including the women, youth and marginalized groups.'[143] Clause 12 of this Bill also requires the creation of affirmative action programmes to ensure that marginalised groups participate in policy formulation and have 'timely access to information.'

Like the Cybercrimes process, the ICT policy and data protection processes were affected by language, access and time challenges which were observed at the pre-formalisation, notification, completion and post-completion stages. The various state agencies failed to issue notices on radio or television prior to the public hearings and to ensure effective and meaningful public participation of all stakeholders.

While some channels for remote participation were provided, this was hinged on effective communication, document management and secretariat capacity by the agency leading the process. For example, during the ICT policy process, one interviewee noted that submissions by email and post, may not have been considered, especially due to a poor secretariat.

Moreover, two dailies - the *Daily Nation* and *The Standard* newspapers - were commonly used by Parliament and state agencies to issue notices for public participation on draft Bills or policies.

These dailies have limited reach across the country and thus leave out those in some urban, remote and rural areas, or those who cannot afford or do not subscribe to them. Various groups were disproportionately affected, including persons with disabilities, illiterate persons, persons without access to the Internet and digital technologies, and persons who are not conversant with English.

Additionally, the failure to publish documents in both national languages (Kiswahili and English) also affected these two processes. For example, the public notices, the draft data protection Bills, the draft ICT policy 2016, and subsequent Committee and Hansard reports, were all issued exclusively in English. There were no concrete efforts made to communicate to the public in Kiswahili or to issue information in accessible formats, which affected Kiswahili speakers and persons with disabilities.

These processes were also impacted by glaring time deficiencies, with stakeholders being provided with either insufficient and disproportionate time for public engagement or lengthy durations without feedback. These challenges affected stakeholders' ability to fully and properly prepare, respond and participate. One interviewee affirmed that timely notice 'has been a big problem across all these processes.'[144] During the consideration of the Data Protection Bill at the National Assembly Committee level, there are written complaints captured in the Committee report decrying the actual time provided to the public to provide comments.

Specifically, one stakeholder 'strongly objected to the very short time for members of the

public to give their views to the matter... it is scandalous and, almost certainly unconstitutional, as well as against the National Assembly's own guidance, to only give three working days (11- 16 July 2019) for contributions.'[145]

The National ICT Policy stewards placed the finalisation of the policy on hold for three-years, during which time, changes were effected in the document, without the input of the Working Groups and the general public, or periodic updates on the progress towards the finalisation of the policy. This left many stakeholders frustrated, and affected stakeholders' ability to contribute to the subsequent iterations of the policy based on new developments, before its publication.

Poor Engagement at the County Level

The failure to hold public engagements at the county level or to properly execute publicised county engagements impeded the openness and accessibility of all three processes, to varying degrees. Instructively, since 2016, only one out of the three processes prioritised public consultation meetings at the county level. During the cybercrimes and the ICT policy processes no public meetings were held outside of Nairobi. This is despite the extensive three-year period from the 'formal' commencement of both processes, to their culmination.

During the consideration of the Data Protection Bill at the National Assembly Committee level, some meetings were held at the county level. The Committee carried out public meetings in 7 out of 9 gazetted counties, excluding Isiolo and Laikipia counties. Neither the exclusion of Isiolo and Laikipia nor the preference of two coastal counties (Mombasa and Kilifi) was not explained in the Committee report.[146]

Lack of Public Participation Legislation

Like the Cybercrimes process, the ICT policy and data protection processes were affected by the absence of a public participation law, or guidelines to standardise public participation. While a Public Participation Bill, 2019 has been published, the failure to subject the Bill to the public participation process and to enact it has resulted in differences in the interpretation and application of public participation by state agencies during the three processes. This denies citizens the opportunity to fully exercise this right and participate in policy and law making processes.

In the data protection and ICT policy processes, this failure created divergence in the manner in which stakeholders presented their submissions owing to the lack of a clear standard or guidelines for public participation, the mode, method and format of making submissions, thus impeding the level of openness and accessibility of the processes.

In other jurisdictions, including New Zealand,[147] Canada,[148] South Africa[149] and Australia,[150] guidelines recognise that content and format are factors that need to be considered carefully to ensure that public submissions are clear, concise, accurate, relevant, evidence-based and effective, to maximize impact during consideration.

3.2.2 Lack of Diversity in Participation

This section assessed the challenges that hindered the processes from being diverse, and the barriers faced in ensuring the different views and interests of the stakeholders were allowed and heard, the limitations faced by stakeholders in contributing, and the level of consideration given to their inputs.

Lowest Scores: ICT Policy Process

Generally, the ICT Policy process was the least diverse. This was primarily due to the failure by the NCS and the ICT Ministry to document and publish stakeholder inputs (whether written and oral), and any other relevant supporting documentation, across all stages of the policy process. The lack of publicly available documentation makes it difficult to identify who the relevant stakeholder groups were, their interests, and the mode (oral or written) of their submissions and the nature of their interest.

Whereas each Working Group received specific comments before and during the Laico public meeting, they did not have further opportunities to properly consider and incorporate the submissions of stakeholders, including those sent by email, because a final meeting to do so was not held.

The failure to have this meeting also denied the Working Groups the opportunity to agree on a consolidated version of the draft Policy. Moreover, the subsequent blackout from 2016 denied the Working Groups and the public an opportunity to contribute further to the ICT Policy development process. One interviewee noted that the ICT Policy process had 'its own owners', namely the ICT Ministry, which usurped the NCS' mandate and failed to safeguard and promote transparency and openness across the whole spectrum of the

process post the Laico meeting.

This assertion is supported by the fact that no reports were issued illustrating which recommendations were received, and from whom, and how exclusion and/or inclusion was promoted before the ICT Policy was published. No reasons were offered for the failure to document, consider or exclude the stakeholder views submitted.

What did not work well across the other two processes?

Limited Diversity of Stakeholders

Like the ICT Policy Process, the cybercrimes and data protection processes faced challenges to ensure diverse representation and participation of all relevant stakeholder groups. A mapping of the stakeholders in both processes revealed that various stakeholders were glaringly absent, including, *inter alia,* the youth, persons with disabilities, children and the elderly, the LGBTQIA+ community, amongst others.

Conversely, established groups and individuals within the ICT sector were well represented, with some of them being granted multiple opportunities (time and platforms) to contribute to the pre-drafting, drafting, review, and finalisation stages. This resulted in the unequal participation of all stakeholders and the domination of the opportunities for participation by some stakeholders.

3.2.3 Unilateral Decision-Making and Poor Consensus and Collaboration

This section assessed the challenges preventing consensus, common purpose, collaboration and decision-making. It also reviewed the barriers to decision-making such as the unwillingness of stakeholders to cede ground and compromise, power imbalances, mistrust and poor relationships.

Lowest Score: Cybercrimes Process

Generally, the cybercrimes process was the least collaborative and consensus-driven process. The lack of common purpose and goal is evident in the disjointed nature in which government agencies developed the draft bills on cybersecurity and cybercrimes.

The first draft Cybercrime and Computer-related Crimes Bill (2014) originated from the ODPP in 2014, followed by the ICT Ministry's Inter-Agency Technical Committee's draft Computer and Cybercrimes Bill (2016), which was later tabled in the National Assembly as the Computer and Cybercrimes Bill (2017), and finally adopted as the Computer Misuse and Cybercrimes Act, 2018.

During this period, the Senate also published the draft Cybersecurity and Protection Bill (2016), while the CA in December 2015, published the draft Kenya Information Communications (Cyber-Security) Regulations 2016 and the draft Kenya Information Communications (Electronic Transactions) Regulations 2016 under the Kenya Information and Communications Act.

As a result of these disjointed processes, the approach adopted and the numerous proposals in the draft Bills were rejected by stakeholders. To a large extent, pushing back against problematic provisions, the approach and glaring gaps in the bills remained the rallying call for stakeholders' engagements with the Bills, rather than the common purpose. One interviewee noted that "there was that rush and so many different processes were happening around the same time around cybersecurity."[151]

In comparison, the cybercrimes process was largely characterised by closed-door relationship building between the government and select stakeholders. For example, one interviewee noted that the 'Inter-Agency Technical Committee was conducted in an extremely closed, rather than an open, manner', and that 'requests to bring other stakeholders on board proved futile' with stakeholders interested in contributing to the process being asked to 'prove their expertise on these issues.'[152]

One interviewee also observed that collaboration between non-government stakeholders was weak. At the legislative levels, another interviewee noted that individual MPs wanted to take 'ownership of the Bill' in order to raise their standing before Parliament and to the general public which may have resulted in back-room negotiations and politics.

Informants noted that entities from one stakeholder group (i.e. government entities) with 'authority and influence had significant power' and promoted unilateral decision-

making. These included the NA Administration and Security Committee, NA ICT Committee and national security agencies.

As one informant noted, the Kenya Police 'were very vocal about them being given greater powers of investigation' under the cybercrimes Bill, while the NA Security Committee proposed several amendments to the Bill at the floor of the house.[153] The substitution of stakeholders' proposals for a multi-stakeholder committee with a one composed exclusively by government representatives only also indicates the attitude of government agencies towards collaboration, consensus and compromise and points to the mistrust of government of other stakeholders.

This also indicates that decisions were not made by general agreement and that government agencies held more weight and power over the decision-making process than others.

As a result, they are problematic as they fail to empower stakeholders with opportunities to contribute and shape narratives, and they take away stakeholders' ability to contest these fixed decisions at the preliminary stages of the deliberations. As one interviewee noted, *'we knew and understood that if we push too hard, we may not have anything in the end or anything we wanted… you go to the table with priorities… if you get at least three things, it's better than nothing… so I let (some crucial issues) go and we (focused) on the big issues.'*[154]

From the foregoing, it is evident that backroom politics, negotiations and the fear of being excluded from future processes informed wanting levels of collaboration in the process.

Some informants expressed a fear of being excluded from future processes, where they either tried to bring other stakeholders into closed processes or where they attempted to address problematic provisions, with the goal of introducing stronger protections or ensuring their complete deletion. Some informants noted that the introduction of new provisions into Bill's or gazetted legislative documents, which were either not subjected to deliberations during the public participation period, or provisions which were rejected unanimously by a majority of stakeholders, created mistrust between the government and other stakeholders.

The institution of a constitutional petition challenging the Computer Misuse and Cybercrimes Act, 2018[155] immediately after its enactment indicates that a common purpose, goal, outputs and milestones were not actively promoted or implemented. Also, it indicates that opportunities for dissent were not practically encouraged or internalised because of the power imbalance in decision-making skewed towards the state.

What did not work well across the other two processes?

Poor Consensus and Collaboration

Like the cybercrimes process, the data protection and the ICT Policy process faced challenges in ensuring collaboration and consensus. The data protection processes was affected by shifting milestones and outputs, coupled with concurrent processes at the various executive and legislative levels.

The introduction of two different Bills by both Houses of Parliament demonstrated the initial failure to agree on a single process guided by a common purpose, milestones and outputs. In turn, this resulted in stakeholders duplicating efforts and wasting stakeholders' time. There was uncertainty among stakeholders as it was also unclear which of the processes would ultimately carry the day. Moreover, the fact that processes in either house were ostensibly guided by different rules, procedures and committees added a further layer of complexity to participation.

At the ICT Policy level, one informant noted that the 'ICT Policy process had 'its own owners which resulted in the NCS, the original policy owner, being usurped and sidelined.'[156] Further, while stakeholders were represented in the multi-sectoral working groups, this same level of ownership, authority, power, compromise and participation disappeared once the document moved from the Working Groups to the ICT Ministry for review and approval.

For example, the three-year blackout not only delayed, but also demonstrated a lack of direction and consensus on the expected milestones and timelines. As one interviewee noted, the intended Working Group meeting in Naivasha intended to provide a collaborative platform for the consolidation of stakeholder submissions and inputs from the Laico meeting never took place. Rather, the NCS and the ICT Ministry single-handedly took charge of the consolidation process, which was not opened again to the public.

The data protection process was marked by the exertion of power, authority and influence by state agencies. One interviewee noted that the Task Force 'did not put in the data localisation' clause into the data protection Bill they generated, but this clause appeared in the versions which were presented before the National Assembly.' The reason for this inclusion remains unclear. Further, backroom politics, private lobbying, and negotiations by local and multinational private sector entities, affected the levels of trust among stakeholders and influenced the trajectory of decision-making within the executive and legislature.

Another interviewee noted that there were attempts by big data and other multinational companies who tried to 'promote the deletion of the localisation requirement' and 'dilute the need to provide for a human review appeal process' by 'directly reach[ing] out to highly-ranked ICT Ministry officials.' These actions 'provided them with an unfair advantage' aimed at influencing the data protection process and the final Bill.' [157]

3.2.4 Limited Evidence for Decision-Making

This section assessed the lack of balanced expertise and research in the processes, and the lack of agreement on the interpretation and use of facts.

Lowest Score: Cybercrimes Process

Generally, the cybercrimes process was the least evidence-based process. Prior to the formation of the Inter-Agency Technical Committee in 2016, the ICT Ministry received input from a very limited group of stakeholders without a public call for stakeholder submissions.

These included the Central Bank of Kenya, Office of the Director of Public Prosecutions, Kenya Law Reform Commission, Communications Authority of Kenya, the National Police Service, National Intelligence Service and Technology Service Providers of Kenya, Directorate of Criminal Investigations, Jomo Kenyatta University of Agriculture and Technology, Strathmore University, Information Communications and Technology Authority, and Media editors.

Subsequently, the Inter-Agency Technical Committee was formed and its membership derived from a few stakeholders, including national security government agencies (CID, CBK), technical bodies (TESPOK), academia (JKUAT and Strathmore) and one CSO (ARTICLE 19 EA). A GPD report noted that various stakeholders had 'insufficient awareness of cybersecurity issues' which was confirmed by interviewee's.

One interviewee noted that 'at the government level, there were few people with expertise and there were also a lot of capacity gaps across all stakeholder groups for people to be allies. Even the human rights commissions that you would have expected to come out strongly on the human rights angle didn't properly understand the importance of digital rights.' Also another interviewee noted that security professionals and ICT experts were glaringly absent from the conversation.

Despite the existence of some baseline research, e.g., the National Cybersecurity Strategy (2014), [158] the cybercrimes Bills did not reflect the wider goals of this Strategy, by singularly focusing on cyber crimes rather than providing a comprehensive cybersecurity framework. Reports by GPD also noted that discourse on cyber security was 'fragmented' with various stakeholders possessing 'insufficient awareness of cybersecurity issues' which resulted in disjointed discourse and efforts, including amongst CSOs. Also, this was also affected by the varying levels of participation of stakeholders in the multiple processes leading up to the Computer Misuse and Cybercrimes Act, 2018.

Lastly, despite the public participation meetings and the provision of oral and written comments by stakeholders, evidence and fact building was superseded by special interests of MPs, including national security. For example, despite objections by stakeholders and by MPs on the floor of the house, the National Assembly retained provisions on 'false publications' which mirror criminal defamation provisions which had been declared unconstitutional in the *Jacqueline Okuta* case.[159] The neglect of stakeholder views contributed to the filing of a petition challenging the constitutionality of the Computer Misuse and Cybercrimes Act, 2018. Further, the weak framework resulted in the Central Bank of Kenya developing cybersecurity guidelines for payment service providers in 2019 ostensibly to address the shortcomings in the law.[160]

What did not work well across the other two processes?

Limited Evidence
Like the cybercrimes process, the data protection and the ICT Policy processes faced challenges in ensuring balanced expertise and research in the processes, and securing agreement on the interpretation and use of facts.

Generally, both processes were not informed by extensive research that was made publicly available to stakeholders. In the data protection process, one interviewee noted that 'the Taskforce conducted research and had scheduled consultative sessions with leading global data protection experts,' but this material was not shared with or made available to all stakeholders, before the public call for stakeholder inputs was announced.[161] The ICT Policy process was informed by limited research located in pre-existing government documents, such as the ICT Masterplan.

The limited research, evidence and facts led to disagreements on the proposals to be included in the Data Protection Bill. For example, despite objections by stakeholders during public participation meetings and in submissions, the National Assembly opted to create a state agency citing budgetary constraints, rather than an independent data protection office, which went counter to the mechanism provided for in previous Bills, and standards set in regional (AU Convention) and international (EU GDPR) laws and standards.

Likewise, calls by stakeholders to clearly define exemption such as 'national security' were ignored. The neglect of stakeholder views contributed to the filing of a petition challenging the constitutionality of the office, the exemptions and the constitutionality of the law generally.

At the ICT policy level, the failure to hold a final Working Group meeting failed to ensure that decisions affecting the draft ICT Policy 2016 were promoted and sanctioned by an expert stakeholder group which had been instrumental in the evidence and fact-gathering process. Lastly, the three year 'black out' meant that new and relevant evidence and facts could not be submitted from the Working Groups or the public in general.

3.2.5 Poor Transparency and Accountability

This section assessed the lack of clearly defined and transparent procedures and mechanisms and the failure to comply with these procedures. It also considered other challenges such as the non-disclosure of stakeholder interests and affiliations; non-existence of clear systems of records management and documentation; and inadequate lines of accountability, both internally (between the leadership and group) and externally (between stakeholders and their wider communities).

Lowest Score: Cybercrimes Process

Generally, the cybercrimes process was the least transparent and accountable. The composition of the Inter-Agency Technical Committee and the rules and procedures governing its operation remained unknown during the entire process, and heralded the opaque and closed nature of the process from its inception. Despite efforts by stakeholders to open the committee membership, and prompts to some committee members to formally disclose their interest and representation, the environment of secrecy and information controls persisted.

Further, the low level of transparency and accountability was exacerbated by the opaqueness of the operations and processes of the Committee; the unilateral decision making of the ICT Ministry; the secrecy of the draft document versions; and lack of information about, and from, the document custodians. As one interviewee noted, during the public participation meeting at Intercontinental Hotel, the ICT Ministry failed to provide stakeholders with hard copies of the Bill. Instead, 'only presentations were prepared by the ICT Ministry which moderated the meeting.'

Further, the National Assembly ICT Committee developed a report of its public participation meetings, but this is not publicly available on Parliament's website. Additionally, the report makes reference to but does not document stakeholders' oral or written submissions either as annexures or as resolutions/ minutes. The standard envisaged in the Public Participation Bill, clause 10 (2) promotes the capturing, documenting and publicising of oral submissions through minutes and

resolutions. Ideally, these should, as a minimum, detail issues raised and resolved during public participation fora.

The lack of a clear roadmap for the legislative process outlining the lead agency resulted in several duplicate processes instituted by multiple state agencies at the Executive and Legislature. This challenge also affected stakeholders' ability to effectively contribute to the processes.

Additionally, the custodians of the draft Bills failed to provide a proper, standardised approach including numbering of the draft documents generated, tracking the changes made in the documents, providing justifications for the amendments, and making the amended versions available publicly. Such actions could have promoted transparency and accountability in the law-making process.

What did not work well across the other two processes?

No Transparency and Accountabilty

Like the cybercrimes process, the data protection and the ICT Policy processes faced challenges. In both processes, no stakeholders formally declared their interests in writing, except for State organs empowered to make law. These formal declarations could have assisted in the promotion of transparency and accountability.

During the ICT policy process, one interviewee noted that the lack of formal declarations was 'problematic especially for the Working Group chair's and members who (may have) approached the process as an opportunity to push a specific agenda.' This issue was also present at the Data Protection Task Force level, which was dominated by government and private sector representatives.

Both processes had poor or non-existent procedures and mechanisms, systems for records and disclosure, and lines of accountability. Crucially, the appointment procedures and the criteria used to select and appoint members of the Data Protection Taskforce and the ICT Policy Working Groups by the ICT Ministry were at the ministry's discretion.

Further, these processes lacked proper record-keeping and document management systems. While noteworthy efforts exist where state agencies attempted to retain records, the existing and fragmented online repositories are not comprehensive as they lack critical documents relating to the processes. For example, the various drafts developed by the ICT Policy Working Groups or the final report of the Data Protection Taskforce are not publicly available. This not only affects the right to information and also prevents the provision of a holistic picture of the ICT processes.

Poor Documentation of Stakeholder Inputs

The data protection and ICT Policy processes failed to properly document stakeholder inputs. Primarily, the responsibility of capturing and documenting stakeholder inputs rests with the secretariat of the state agency responsible for the process.

In the data protection process, one informant noted that some submissions, especially electronic submissions, 'may not have been considered by the (data protection) Taskforce, especially where an inattentive secretariat existed.'[162]

Further, there was a divergence in reporting revealing that transparency and accountability was not prioritised across all stages. Despite the availability of a National Assembly ICT Committee report which can be accessed in electronic format on Parliament's website, the same level of reporting was not replicated at the Task Force level.

Despite the NA Committee report attaching stakeholders' written submissions as annexures to the report, this same level of documentation was not replicated for oral submissions, making it difficult to assess stakeholder inputs fully. In the ICT Policy process, the ICT Ministry and the NCS failed to provide each Working Group with a secretariat to support the capturing and consolidation of stakeholders' submissions.

One interviewee confirmed that the Working Groups faced budgetary constraints and had to 'source their own secretaries.'[163] Further, the Working Group reports and stakeholders' submissions are not available online. It is also unclear how and whether stakeholders' written and oral submissions were considered by the ICT Ministry after the public participation process, and whether these informed the ICT Policy 2019.

4.0 Conclusion and Recommendations

This study has assessed the extent to which the public was informed, consulted and involved in the processes leading to the development of the National Information Communications and Technology (ICT) Policy, 2019; the Computer Misuse and Cybercrimes Act (2018); and, the Data Protection Act, 2019.

Based on the 'Diagnostics Tool for Inclusive Cyber-Policy Making,' the report reviewed the extent to which each process was 'open and accessible', 'diverse', 'collaborative', 'consensus-driven', 'evidence-based', and 'transparent and accountable'.

Further, it highlights specific challenges which constrained the processes including the limited openness and accessibility; lack of diversity in participation; unilateral decision-making and poor consensus and collaboration, limited evidence for decision-making; and, poor transparency and accountability.

These challenges indicate that the transition to a more participatory, transparent, democratic, multi-stakeholder approach in ICT policy-making still falls below the standard envisaged in the Constitution of Kenya, 2010. Two of the processes reviewed were immediately challenged in court by stakeholders who participated in the public process, but were aggrieved by state agency failures to provide adequate, transparent and accountable mechanisms for public participation.

Further, the continued delay to enact the Public Participation Bill, 2019 has resulted in differences in the interpretation and application of public participation by state agencies, thus denying citizens the opportunity to fully exercise this right.

As evidenced above, implementing the principle of public participation under Article 10 of the Constitution, 2010 in ICT policy and law-making can better be achieved by compliance with the principles of the multistakeholder model. Based on the foregoing, we recommend the following:

1. General

a. The National Assembly should update and enact the Public Participation (No. 2) Bill, 2019. The Bill should provide principles for public participation, guidelines to the public for making oral and written submissions, prescribe standards and procedures for submissions, and set timelines for consideration and feedback.
b. The Judiciary should urgently conclude the constitutional petitions affecting the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act, 2019.
c. The Commission on Administrative Justice should develop guidelines for all public entities to facilitate the disclosure of information relating to policy and law-making processes.

2. Open and accessible

a. State agencies should issue public notices, draft Bills or policies, Committee and Hansard reports in both official languages (Kiswahili and English).
b. State agencies should use radio, TV and social media platforms to ensure meaningful and effective public participation and the engagement of all stakeholders, especially those in some urban, remote and rural areas, or those who cannot afford or do not subscribe to local daily newspapers.
c. State agencies should give at least twenty-one (21) days notice of public participation processes, and include details of contact persons, a summary of questions being released for public consultation, a standardised format of submissions, deadlines for receipt of memoranda, and the means through which to make submissions, such as email, post or physical addresses.
d. State agencies should convene public participation fora at the county level.
e. State agencies should provide opportunities for remote participation during public participation meetings, including through video conferencing solutions or online feedback platforms.

3. Diverse

a. State agencies should proactively engage more 'non-traditional' stakeholders, including marginalised and minority groups such as rural communities, youth, students, children, the elderly, persons with disabilities, and the LGBTQIA+ community.
b. State agencies should treat all stakeholders fairly and grant them equitable audience.
c. State agencies should consider all stakeholder submissions, and give feedback to the public, within a reasonable period, on their consideration and justifications for the inclusion or exclusion of submissions.
d. State agencies should publish all stakeholder submissions and the agencies feedback on the submissions on publicly available platforms.

4. Collaborative and Consensus-driven

a. State agencies addressing a common policy issue, should collaborate with each other and agree on a common purpose and goal with stakeholders to avoid confusion and duplication of policy and law-making processes.
b. State agencies should prioritise collaboration and consensus building with stakeholders to promote trust, from the commencement to the finalisation of policy and law-making processes.
c. State agencies should promote decision-making by general agreement and consensus, and address the power imbalances within the various stakeholder groups.
d. State agencies should provide stakeholders with reasonable opportunities to openly contribute and shape narratives, and restrict backroom lobbying, deliberations and negotiations.

5. Evidence-based

a. State agencies should conduct extensive and objective background, issue and evidence-based research prior to developing policies and laws and avail the research publicly to all stakeholders to provide a baseline level of evidence and facts.
b. State agencies should ensure that policy documents are in place prior to the commencement of legislative processes, and ensure that draft laws reflect the goals set out in these documents.
c. State agencies should allocate sufficient space and time to discuss and interpret opinions, facts and evidence on public policy issues.
d. State agencies should consult diverse subject matter experts during policy and legislative processes.
e. State agencies should ensure that special interests (political, business and security) do not override stakeholders' input, evidence and facts.

6. Transparent and accountable

a. State agencies should require all participating stakeholders to clearly disclose their name, identify their stakeholder grouping, formally declare their interest, and specific issue(s) being addressed.
b. State agencies should prepare and publicly avail, in partnership with stakeholders, a guiding document(s) outlining formal procedures and mechanisms prior to the commencement of a process. This document should clearly set out the leadership, representation of the stakeholders, rules of engagement and process for contribution, inclusion and exclusion of inputs, decision-making powers and methods, accountability and redress.
c. State agencies should disclose the appointment procedures and criteria used to select and appoint members to quasi-administrative bodies (e.g., committees and Taskforces) created to increase the efficiency of the legislative process.
d. State agencies should create functioning, accessible and regularly maintained online and offline record management systems containing all documentation affecting an ICT and law-making process.
e. State agencies should provide clear avenues for redress capable of promoting accountability and proper dispute resolution.

Endnotes

1. Exploring the multi-stakeholder experience in Kenya https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1249898
2. Public Participation Bill (No.2) 2019 http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/PublicParticipation_No._2_Bill_2019.PDF
3. Tunis Agenda for the Information Society http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
4. WSIS+10 Statement on the Implementation of WSIS Outcomes http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf
5. NETmundial Multistakeholder Statement https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
6. Ibid
7. A stakeholder refers to an individual, group or organization that has a direct or indirect interest or stake in a particular organization; that is, a given action has the ability to influence the organization's actions, decisions and policies to achieve results.
8. Multistakeholder Model https://icannwiki.org/Multistakeholder_Model
9. Ibid
10. NETmundial Multistakeholder Statement https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
11. Framework For Multistakeholder Cyber Policy Development https://www.gp-digital.org/publication/multistakeholder-framework/
12. Framework For Multistakeholder Cyber Policy Development https://www.gp-digital.org/publication/multistakeholder-framework/
13. National Information Communications Technology (ICT) Policy, pp. 3 https://ca.go.ke/wp-content/uploads/2018/02/The-ICT-Sector-Policy-Guidelines-of-March-2006.pdf
14. Telecommunications and Postal Sector Statement, December 2001. https://ca.go.ke/wp-content/uploads/2018/02/Telecommunications-and-Postal-Sector-Guidelines-of-December-2001.pdf
15. *Ibid.,* Foreword.
16. Ibid., Foreword.
17. There are reports which noted that Kenya's first national ICT policy was actually released in late 2003, before the World Summit on the Information Society (WSIS) in Geneva. The copy was however not officially available and was more of a document just to give Kenya face during the world summit.' See: Kandiri, J 'ICT policy in Kenya and ways of improving the existing ICT Policy,' pp. 14. https://su-plus.strathmore.edu/bitstream/handle/11071/3638/ICT%20policy%20in%20Kenya.pdf?sequence=1&isAllowed=y
18. National Information Communications Technology (ICT) Policy https://ca.go.ke/wp-content/uploads/2018/02/The-ICT-Sector-Policy-Guidelines-of-March-2006.pdf
19. Exploring the multi-stakeholder experience in Kenya https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1249898
20. *Ibid.,*
21. National Information Communications Technology (ICT) Policy, pp. 2 https://ca.go.ke/wp-content/uploads/2018/02/The-ICT-Sector-Policy-Guidelines-of-March-2006.pdf
22. Republic of Kenya (2014) 'The Kenya National ICT Masterplan 2014 - 2017 http://icta.go.ke/national-ict-masterplan/
23. National Broadband Strategy http://icta.go.ke/the-national-broadband-strategy/
24. National Cyber Security Strategy (2014) http://icta.go.ke/national-cyber-security-strategy/
25. Republic of Kenya (2014) 'The Kenya National ICT Masterplan 2014 - 2017 http://icta.go.ke/national-ict-masterplan/
26. Ibid
27. CIO, East Africa (2016) 'Draft on Kenya's ICT Policy now ready for stakeholders validation.' https://www.cio.co.ke/draft-on-kenyas-ict-policy-now-ready-for-stakeholders-validation/
28. ICT Wishlist #FIRST100Days https://www.kictanet.or.ke/?mdocs-file=40199
29. Wainaina, E (2016) 'ICT Ministry is Seeking your input on the National ICT Policy 2016. https://techweez.com/2016/03/17/national-ict-policy-2016/
30. ICT Ministry bets on policy review to grow https://www.standardmedia.co.ke/index.php/amp/sci-tech/article/2000195755/ict-ministry-bets-on-policy-review-to-grow-sector
31. Ibid
32. New ICT Sector Guidelines Due By June 2016 https://www.capitalfm.co.ke/business/2016/03/new-ict-sector-guidelines-due-by-june-2016/
33. KEPSA 'Kenya National ICT Sector Policy Guide-

lines 2006 Review.' https://kepsa.or.ke/13597-2/
34. KII interview, October 2020
35. Republic of Kenya (2016), Draft National ICT Policy 2016. http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf
36. *Ibid*., n. 58. pp. 13. Also: Wainaina, E (2016) 'Kenya's ICT Ministry is Seeking your input on the National ICT Policy 2016.' https://techweez.com/2016/06/21/ict-policy-2016/
37. Kenya ICT Action Network (2016) 'Annual Report,' pp. 14. https://www.kictanet.or.ke/wp-content/uploads/2017/09/KICTANet_Annual_Report_2016.pdf
38. KEPSA (2016) 'National ICT Policy Awaiting Cabinet Approval.' https://kepsa.or.ke/news/national-ict-policy-awaiting-cabinet-approval/; ICT Ministry (2016) 'Draft ICT policy set for Cabinet approval.' https://ict.go.ke/draft-ict-policy-set-for-dabinet-approval/
39. ICT Ministry (2017) 'Government reviewing ICT policy.' https://ict.go.ke/government-reviewing-ict-policy/;
40. Abuya, K (2019) 'Kenya ICT Ministry concludes review of the National ICT Policy.' https://techweez.com/2019/10/14/national-ict-policy-review/
41. KICTANet (2020) 'National ICT Policy 2019.' https://www.kictanet.or.ke/national-ict-policy-2019-2/
42. Republic of Kenya (2019) 'National ICT Policy, 2019.' https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf
43. Key Informant interview, October 2020
44. Ministry of ICT, Innovation and Youth Affairs, Twitter https://twitter.com/MoICTKenya/status/1211875062783135746?s=20
45. The Kenya Gazette (2020) Vol. CXXII—No. 150, 'The National Information Communications and Technology (ICT) Policy Guidelines, 2020,' pp. 3064. http://kenyalaw.org/kenya_gazette/gazette/volume/MjE5Nw--/Vol.CXXII-No.150/
46. Republic of Kenya (2013) 'Kenya Information and Communication Amendment Act (2013).' https://ca.go.ke/document/kenya-information-and-communication-amendment-act-2013-2/
47. Communications Authority of Kenya 'Cyber Security Overview.' https://ca.go.ke/industry/cyber-security/overview/
48. CA (2018) 'Public notice: Key changes in the ICT Sector Law.' https://ca.go.ke/wp-content/uploads/2018/01/Key-Changes-in-the-ICT-sector-Law.pdf
49. Republic of Kenya (2014) 'Cybercrime and Computer related Crimes Bill, 2014.' https://bit.ly/1H0PICH; ODPP (2017) 'Strategic Plan 2016-2021: Figure 1 presents the ODPP Organization chart.' http://www.odpp.go.ke/wp-content/uploads/2017/03/STRATEGIC-PLAN-2016-2021.pdf
50. ARTICLE 19 (20) 'Legal Analysis: Kenya: Cybercrime and Computer Related Crimes Bill.' https://bit.ly/1H0PICH
51. ICT Ministry (2014) 'National Cyber Security Strategy.' pp. 7. http://icta.go.ke/national-cyber-security-strategy/
52. Republic of Kenya (2014) 'The Kenya National ICT Masterplan 2014 - 2017.' http://icta.go.ke/national-ict-masterplan/; UNIDIR Cyber Policy Portal 'Kenya.' https://unidir.org/cpp/en/states/kenya
53. ARTICLE 19 (2016) 'Kenya: Information Communications (Cybersecurity) and (Electronic Transactions) Draft Regulations.' https://www.article19.org/data/files/medialibrary/38413/Kenya-Cyber-Security-and-Electronic-Transactions-Legal-Analysis-21-April-2016.pdf
54. ARTICLE 19 (2016) 'Kenya: Information Communications (Cybersecurity) and (Electronic Transactions) Draft Regulations.' https://www.article19.org/resources/kenya-information-communications-cybersecurity-and-electronic-transactions-draft-regulations/
55. TESPOK, Facebook https://www.facebook.com/Tespok/posts/the-critical-infrastructure-protection-bill-and-draft-policy-is-now-available-fo/764655716990375/
56. Republic of Kenya (2016) '15.1.2 Policy Objectives, Draft National ICT Policy 2016,' pp. 34 - 35. http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf
57. Ibid
58. Republic of Kenya (2016) 'Cyber Security and Protection Bill.' http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2016/CyberSecurityandProtectionBill_2016.pdf
59. Kenyanito, E (2016) 'Testimony about the Cyber Security and Protection Bill before the Kenyan Senate ICT- Committee.' https://ekenyanito.com/2016/10/19/senate2016-cybertestimony/
60. Privacy International (2019) 'State of Privacy Kenya.' https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#data-protection>
61. Input was received from the 'Central Bank of Kenya, Office of the Director of Public Prosecutions, Kenya Law Reform Commission, Communications Authority of Kenya, the National Police Service, National Intelligence Service and Technology Service Providers of Kenya, Directorate of Criminal Investigations, Jomo Kenyatta University of Agriculture and Technology, Strathmore University, Information Communications and Technology Authority, National Communications Secretary and the Ministry of ICT.' See: OpenNet Africa (2016) 'Computer and Cyber Crimes Bill 2016: Government Calls for Public

Participation.' https://www.opennetafrica.org/computer-and-cyber-crimes-bill-2016-government-calls-for-public-participation/

62. CA (2018) 'Public consultation on the Computer and Cybercrimes Bill 2016.' https://ca.go.ke/public-consultation-on-the-computer-and-cybercrimes-bill-2016/
63. Global Partners Digital, Mapping the Cyber Policy Landscape: Kenya https://www.gp-digital.org/publication/mapping-the-cyber-landscape-kenya/;
64. Ministry of ICT 'Cabinet Approves Cyber security Bill.' https://ict.go.ke/cabinet-approves-cyber-security-bill/; TESPOK (2017) 'Request for proposals: Terms of reference (TOR) for a research consultant to develop a policy brief to inform policy and advocacy on the impact of Computer and Cyber Crimes Bill, 2016.' https://www.tespok.co.ke/?page_id=12054
65. Kenya Law 'National Assembly Bills 2017, The Computer and Cybercrimes Bill, 2017.' www.kenyalaw.org/kl/index.php?id=6819
66. Hon. Kisang: Hansard Report (2018) pp. 18. http://www.parliament.go.ke/sites/default/files/2017-05/Hansard_Report_-_Wednesday_21st_March_2018P.pdf
67. *Ibid.,* pp. 11 - 12. These stakeholders included the Media Council of Kenya, the Kenya ICT Action Network, the Centre for Intellectual Property and Information Technology Law, the Communications Authority of Kenya, the Ministry of ICT, the Kenya Private Sector Alliance (KEPSA), the Information Communication Technology Association of Kenya (ICTAK), SOTE Hub, the Information System Audit and Control Association (ISACA- Kenya Chapter), the Technology Service Providers of Kenya (TESPOK), Safaricom Limited, ARTICLE 19 and Mr. Michael Otieno. The Departmental Committee on Administration and National Security presented amendments to the NA Committee.
68. Hon. Kisang: Hansard Report (2018) pp. 11. http://www.parliament.go.ke/sites/default/files/2017-05/Hansard_Report_-_Wednesday_21st_March_2018P.pdf
69. National Assembly (26 April 2018) 'Official Report' pp. 20. http://www.parliament.go.ke/the-national-assembly/house-business/hansard
70. Rödl & Partner (2018) 'Kenya: The Computer Misuse and Cybercrimes Act.' https://www.roedl.com/insights/kenya-computer-misuse-cybercrime-act
71. Hon. Kisang: Hansard Report (2018) pp. 11. http://www.parliament.go.ke/sites/default/files/2017-05/Hansard_Report_-_Wednesday_21st_March_2018P.pdf
72. Hon. Duale: Hansard Report (2018) pp. 10. http://www.parliament.go.ke/sites/default/files/2017-05/Hansard_Report_-_Wednesday_21st_March_2018P.pdf
73. Sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 & 53 of the Computer Misuse and Cybercrimes Act, 2018.
74. Petition 206 of 2019 - Kenya Law, para 136.
75. *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191276/
76. High Court nullifies 23 bills passed by National Assembly without Senate input https://www.the-star.co.ke/news/2020-10-29-high-court-nullifies-23-bills-passed-by-national-assembly/
77. Petition 284 & 353 of 2019 (Consolidated) - Kenya Law
78. Ministry of Information & Communications (2009) 'Data Protection Bill.' https://www.ifex.org/kenya/2011/11/09/kenya_article19_data_protection_bill_final.pdf
79. National Assembly of the Republic of Kenya (2019) 'Report on the Consideration of the Data Protection Bill, 2019,' Annexure 1. http://parliament.go.ke/sites/default/files/2019-10/Report%20on%20Data%20Protection%20Bill%2C%202019_compressed.pdf
80. Ibid, at pp. 155.
81. Republic of Kenya (2013) 'Data Protection Bill.' http://icta.go.ke/data-protection-bill-2012/
82. Privacy International and the National Coalition of Human Rights Defenders in Kenya (NCHRD-K) (2014), pp. 13. https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=1420&file=CoverPage
83. KICTANet (2018) 'Policy Brief: Data Protection in Kenya.' https://www.kictanet.or.ke/download/data-protection-in-kenya/; National Assembly Bills 2014 http://kenyalaw.org/kl/index.php?id=4250; National Assembly Bills 2013 http://kenyalaw.org/kl/index.php?id=4251
84. National Payment Systems Act https://www.centralbank.go.ke/images/docs/legislation/NATIONAL%20PAYMENT%20SYSTEM%20ACT%20(No%2039%20of%202011)%20(2).pdf
85. Consumer Protection Act (2012), http://www.parliament.go.ke/sites/default/files/2017-05/ConsumerProtectionActNo46of2012.pdf
86. Kenya Information and Communications Act (KICA) (2012) https://www.unodc.org/res/cld/document/ken/1930/information-and-communications-act_html/Kenya_Information_and_Communications_Act_2_of_1998.pdf
87. Consumer Protection Regulations (2010) http://kenyalaw.org/LegalNotices/pop_ln.php?file=392
88. Registration of SIM-Cards Regulations (2015) http://kenyalaw.org/kl/fileadmin/pdfdown-

loads/LegalNotices/163-Kenya_Information_and_Communications_Act__Registration_of_Sim-Cards__Regulations__2015.pdf

89. Access to Information Act (2016). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016
90. Key informant Interview, October 2020
91. Section 21 (1) (a - h), Access to Information Act (2016). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016
92. National Assembly of the Republic of Kenya (2019) 'Report on the Consideration of the Data Protection Bill, 2019,' Annexure 1. http://parliament.go.ke/the-national-assembly/committees/12/communication-information-innovation
93. Senate Bills (2018) 'Data Protection Bill, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2018/DataProtectionBill_2018.pdf
94. *Ibid*., 'Memorandum of Objects and Reasons', pp. 330.
95. The Kenya Gazette, Vol. CXX - No. 56 (2018) 'Gazette Notice No. 4367.' http://kenyalaw.org/kenya_gazette/gazette/volume/MTcwNg--/Vol.CXX-No.56/
96. Ministry of ICT (2018) 'Privacy and Data Protection Policy 2018 – Kenya.' http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf
97. Ministry of ICT (2018) 'The Data Protection Bill 2018 – Kenya.' http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf
98. Hussain, A (2018) 'Kenya: Data Protection Bill "a step in the right direction but in need of substantial review." https://corporate.dataguidance.com/kenya-data-protection-bill-a-step-in-the-right-direction-but-in-need-of-substantial-review/
99. KBC Channel 1 (2018)'Task-force to compile report that will inform storage of data.' https://www.youtube.com/watch?v=OIKLvblzK-k&feature=youtu.be&t=28
100. Ministry of ICT 'Request for comments on the Proposed Privacy and Data Protection Policy and Bill, 2018.' https://ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/; Communications Authority of Kenya (2018) 'Request For Comments On The Proposed Privacy And Data Protection Policy And Bill, 2018.' https://ca.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/; Ministry of ICT, CA New 16X3 (13-9).
101. Issaias, A & Syekei, J (2018) 'Taskforce to finalise data protection bill after reviewing all public comments.' https://www.bowmanslaw.com/insights/intellectual-property/taskforce-to-finalise-data-protection-bill-after-reviewing-all-public-comments/
102. Key Informant Interviews, October 2020
103. Otieno, J (2019) 'CS Mucheru, senators strike deal on data protection bill.' https://www.the-star.co.ke/news/2019-05-09-cs-mucheru-senators-strike-deal-on-data-protection-bill/
104. State House Kenya (2019) https://twitter.com/StateHouseKenya/status/1118877236201963521
105. Ayega, D (2019) 'National Assembly role in Data Protection Bill lands Mucheru in trouble with Senate.' https://www.capitalfm.co.ke/news/2019/06/national-assembly-role-in-data-protection-bill-lands-mucheru-in-trouble-with-senate/
106. Data Protection Bill, 2019 http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/TheDataProtectionBill_2019.PDF
107. Ayega, D (2019) 'National Assembly role in Data Protection Bill lands Mucheru in trouble with Senate.' https://www.capitalfm.co.ke/news/2019/06/national-assembly-role-in-data-protection-bill-lands-mucheru-in-trouble-with-senate/
108. Ibid.
109. Senate Bills 2018 http://kenyalaw.org/kl/index.php?id=7937
110. Specifically, three Senators, including Senators Ledama Ole Kina (Narok), Enock Wambua (Kitui) and Halake Habisori 'said they will not accept the new development.' Ibid.
111. National Assembly Bills - 2019 http://kenyalaw.org/kl/index.php?id=9091
112. National Assembly of the Republic of Kenya (2019) 'Report on the Consideration of the Data Protection Bill, 2019,' pp. 5. http://parliament.go.ke/the-national-assembly/committees/12/communication-information-innovation
113. Ibid
114. Data Protection Act (No. 24 of 2019) http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
115. Immaculate Kassait appointed as Kenya's first Data Commissioner https://www.kbc.co.ke/immaculate-kassait-appointed-as-kenyas-first-data-commissioner/;
116. Section 7 (2), Data Protection Act (2019) http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019
117. Court declines to suspend Data Protection Act https://www.the-star.co.ke/news/2019-11-21-court-declines-to-suspend-data-protection-act/
118. Mombasa and Nakuru County public forum meetings - NA Committee report. pp. 35 & 38)
119. Key Informant Interviews, October 2020
120. Key Informant Interviews, October 2020
121. Key Informant Interviews, October 2020

122. Republic of Kenya (2014) 'The Kenya National ICT Masterplan 2014 - 2017' pp 21, http://icta.go.ke/national-ict-masterplan/
123. Key Informant Interviews, October 2020
124. Key Informant Interviews, October 2020
125. Key Informant Interviews, October 2020
126. Key Informant Interviews, October 2020
127. Key Informant Interviews, October 2020
128. AptanTech (2017) 'ESET to set up research and cyber-security operations centre at Strathmore University.' https://aptantech.com/2017/03/eset-to-set-up-research-and-cyber-security-operations-centre-at-strathmore-university/
129. AIRA, About Us https://aira.africa/about-us/
130. Key Informant Interviews, October 2020
131. Ibid.
132. Key Informant Interviews, October 2020
133. Key Informant Interviews, October 2020
134. Key Informant Interviews, October 2020
135. Published Findings https://ca.go.ke/consumers/public-consultations/published-findings/
136. National Assembly of the Republic of Kenya (2019) 'Report on the Consideration of the Data Protection Bill, 2019.' parliament.go.ke/sites/default/files/2019-10/Report on Data Protection Bill%2C 2019_compressed.pdf
137. Key Informant Interviews, October 2020
138. Access to Information Act, section 5; available at: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016
139. Means any public office, as defined in Article 260 of the Constitution; or any entity performing a function within a commission, office, agency or other body established under the Constitution. Section 2 of the Access to Information Act, 2016
140. Ibid, section 5 (2).
141. Ibid, section 5 (3)(c).
142. Key Informant Interviews, October 2020.
143. Section 10, The Public Participation (No. 2) Bill, 2019, http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/PublicParticipation_No._2_Bill_2019.PDF
144. Key Informant Interviews, October 2020.
145. NA Committee Report, (Cybercrimes) Karanja Mutindi, pp. 56.
146. One interviewee rightly noted, in relation to the cybercrimes process, 'when you limit participation, you limit voices.' This section steers away from speculating about the type of contributions which county stakeholders outside of Nairobi would have provided. However, these stakeholders would have introduced 'perspectives which would have enriched the conversation' given the recognition that 'different counties have their different interests and issues.'
147. Making a submission to the parliamentary select committee https://www.parliament.nz/media/2019/makingasubmission2012-2.pdf
148. Guidelines for submitting briefs to House of Commons Committees https://www.ourcommons.ca/About/Guides/brief-e.html
149. Submissions https://www.parliament.gov.za/submissions
150. Making a written submission to a parliamentary Committee https://www.parliament.vic.gov.au/images/stories/WrittenSubmissionA4_2.pdf
151. Key Informant Interviews, October 2020
152. Key Informant Interviews, October 2020
153. Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR http://kenyalaw.org/caselaw/cases/view/191276/
154. Key Informant Interviews, October 2020
155. The rejection of these provisions is succinctly detailed in the constitutional petition contesting 26 provisions in the CMCA (2018), and the Data Protection Petition contesting the operationalisation of a partly independent data protection authority.
156. The NCS draws its mandate from section 84 of the Kenya Information and Communication Act, 1998 and is tasked with 'advising the Government on the adoption of a communication policy.'
157. Key Informant Interviews, October 2020
158. National Cybersecurity Strategy 2014 https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf
159. Hon. Ng'ongo stated: 'This Bill has a provision that outlaws false publication. I know the world today is so concerned with fake news. It is the inthing. It is what is now being discussed. Probably, this Bill will help fight this menace. This idea may be good, but there is a red alert that this offence is similar to the old crime of criminal defamation, which has since been declared unconstitutional.' National Assembly, Official Report, 21 March 2018 Microsoft Word - Hansard Report - Wednesday, 21st March, 2018(P).doc (parliament.go.ke)
160. CBK, Guideline on Cybersecurity for Payment Service Providers, July 2019, https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf
161. Background research - including cost benefit and human rights impact assessments - is crucial for policy and legislative processes, and offers stakeholders with baseline information capable of heightening capacity and knowledge, including international best practices and standards.
162. Key Informant Interviews, October 2020
163. Key Informant Interviews, October 2020

Thank you

We would like to say Thank You, to everyone who made this report a success. We truly appreciate the effort and time you took to contribute and participate in it. We enjoyed and really appreciated you participation."

KICTANet

The Power of Communities

www.kictanet.or.ke