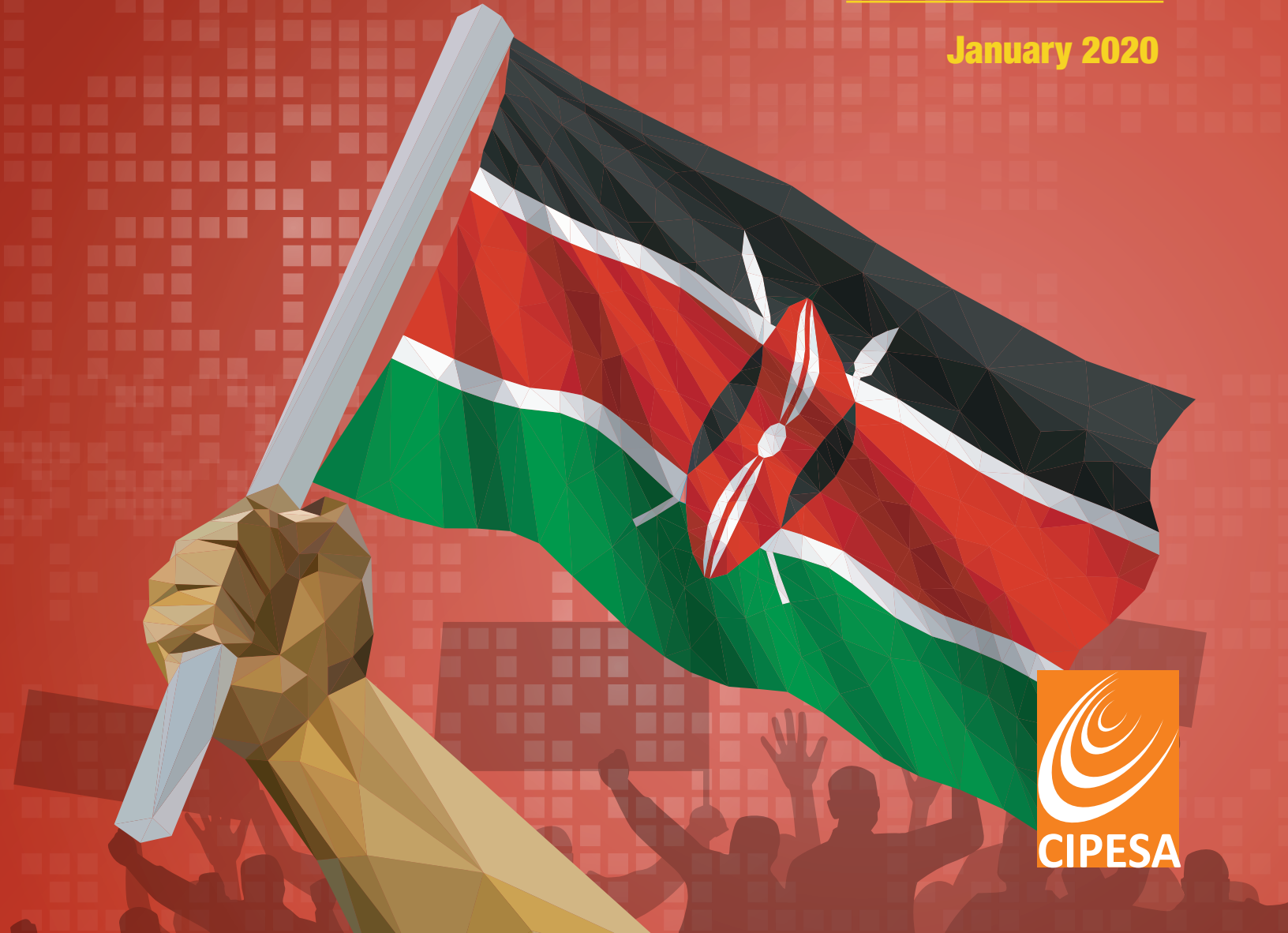
State of Internet Freedom in Kenya 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020



CIPESA

Table of Contents

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Kenya tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Bostwana, Burundi, Cameroon, Chad, the DRC, Ethiopia, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Kenya ICT Action Network (KICTANet) as the main content contributor to this report.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Kenya 2019
Published by CIPESA,
www.cipesa.org
January 2020

1 Introduction

1.1 Introduction

Internet freedom in Kenya has experienced both growth and repression over the last ten years. Successive governments in Kenya have undertaken censorship, surveillance, big data collection and curtailed internet freedom including through the adoption of repressive legislation and practices such as network disruptions and throttling. Key shifts in the internet landscape in the country can be attributed to factors such as the promulgation of the 2010 Constitution of Kenya, the liberalisation of the telecommunications sector, the leadership of the Ministry of Information and Communication Technology (ICT), and global technology policy developments such as the European General Data Protection Regulation (GDPR). Other factors have also included digital migration, the increased use of big data, the socio-political space for freedom of expression, elections, election-related violence, terrorist attacks and private sector initiatives.

While the government has acknowledged the place of ICT as a central pillar to economic development, the measures to control the use of the internet remain of concern. Moreover, social media has emerged as the battlefield where the government has sought to control information, including through retrogressive practices such as spreading propaganda, diverting public attention through misleading stories, spreading fake news and muzzling of critics. Kenya, like many other developing countries, is taking a more active role in global discourses on regulating the digital economy. As more people get online and the government and businesses digitalise, democracy and internet rights are at risk of being eroded if the corporate abuses and state excesses online go unchecked.

To develop a more comprehensive understanding of the on-going discussions around internet freedom, this study will situate these issues against an in-depth trends analysis of how government policies and practices have shaped and impacted on internet freedom in Kenya over the last 20 years. This study therefore presents a broad picture of the evolution of internet freedom in Kenya since the year 2000. It traces the key developments, motivations, effects and impacts of policy decisions and actions on internet freedom in Kenya with a view to analyse the trends of the past so as to make recommendations for the future.

1.2 Aim of the study

This research seeks to document how government controls have affected internet freedom in Kenya since 1999. Specifically, it traces the trends, developments and milestones from 1999 to 2019, as well as drivers of these trends. The study focuses on a select set of issues including the proliferation of retrogressive or repressive policies and laws; surveillance and surveillance capacity of governments; digitisation programmes; censorship; and the new frontiers such as the introduction of internet-related taxes. The findings will inform policy makers, the media, academia, technologists, civil society and other researchers on the policy, legal, institutional and practice landscape with a view to identify opportunities for fostering internet freedom in Kenya.

2 Methodology

This study employed qualitative research methods. Qualitative research was considered most appropriate because in large part the research seeks to discover the correlation between policy and legal frameworks governing Kenya's ICT sector and the state of internet freedom in the country. Specifically, the study analysed the country's policy and legal frameworks governing the ICT sector. Among others, these documents include the Kenya Information and Communications Act, the Computer Misuse and Cybercrimes Act, the National ICT Policy, reports by civil society organisations, and news reports. The study also reviewed international instruments that Kenya is party to as well as relevant constitutional provisions promoting Internet freedom.

In addition, the study engaged key informants including persons in public and private institutions and companies. These include those from the ICT sector, including the sector regulator, Communications Authority, service providers and telecommunication companies such as Safaricom, members of the media, bloggers, academics, human rights defenders, and legal experts.

3 Country Context

This section provides an overview of the ICT sector in Kenya and looks at the political environment and the factors affecting or hindering democratisation in the country. It also provides a brief overview of the country's economy.

3.1 ICT Status

The uptake of ICT in the country has been on a steady rise. The number of mobile phone users grew from 330,000[1] in 2000 to 40,259,476 in 2019.[2] The number of internet users in the country grew in tandem with the number of mobile phone users, from 200,000[3] in 2000 to 43.3 million.[4] This rapid growth also saw the decline of fixed telephone lines over the years as cellular phones disrupted the market. From only nine base stations in 1995 covering only the capital's Nairobi city centre, coverage today is nationwide, reaching 90% of the population.

In 1999, the monopoly of the Kenya Post and Telecommunications Corporation ended, leading to the opening up of the market and the formation of the Communications Commission of Kenya (now the Communications Authority of Kenya (CA),[5] and the emergence of private telecom operator Safaricom. In 2007, Telkom Kenya's monopoly on international gateway ended, bringing down a key barrier to internet access. From 2009, several submarine fibre optic cables were introduced, while international gateways were liberalised, last and first mile solutions were implemented, and telecommunications services converged. The government invested in the development of international and national fibre optic cable routes, supported the development of data centres, and intervened to reduce internet access costs by eliminating certain taxes.

The Communications Authority (the industry regulator) and the Ministry of ICT remain the two main government agencies responsible for ICT policy development, implementation and regulation. Other relevant agencies include the Competition Authority[6] and the Media Council of Kenya,[7] whose roles sometimes overlap with that of the sector regulator, causing confusion and conflict over mandates.

1 *Annual report of the Board for the Financial year 2000/2001, https://ca.go.ke/wp-content/uploads/2018/02/Annual-Report-for-the-Financial-Year-2000-2001.pdf*
2 *Annual Report for the financial year 2016-2017, https://ca.go.ke/wp-content/uploads/2018/04/Annual-Report-for-the-Financial-Year-2016-2017.pdf*
3 *Kenya Internet Usage Stats and Market Reports, https://www.internetworldstats.com/af/ke.htm*
4 *Kenya Telecommunications Reports, https://www.internetworldstats.com/af/ke.htm*
5 *Communications Authority of Kenya, https://ca.go.ke/*
6 *Competitions Authority of Kenya, https://www.cak.go.ke/*
7 *Media Council of Kenya, https://www.mediacouncil.or.ke/en/mck/*

3.2 Political Environment

Kenya has enjoyed relative stability since 1999, save for the 2007 post-election violence that erupted following the disputed 2007 presidential election.[8] The country is ranked by the Economist Intelligence Unit's Democracy Index as a hybrid democracy, meaning it has elements of democracy but also has some flaws including a history of regular electoral fraud; government pressure on the political opposition, non-independent judiciaries, widespread corruption, harassment and pressure on the media, anaemic rule of law, an underdeveloped political culture, and low levels of participation in politics. This puts Kenya at par with countries such as Nigeria, Sierra Leone, and the Gambia.

The internet is not only seen as a tool for socio-economic growth but also as a key instrument for consolidating political power and control. Technology has been deployed during elections to facilitate electronic voter registration, identification, and results tallying. The country has a vibrant online community, with widespread usage of social media for activism, political participation and expression.

However, reports show the use of telecommunication surveillance to monitor the activities of human rights defenders.[9] Likewise, the government is reported to have implemented problematic practices such as the use of bots and propaganda on social media to influence elections and public opinion,[10] as well as intimidation and arrests of critics and bloggers in a bid to strengthen its control over information shared online.[11]

3.3 Economic status

Kenya's recognition of the internet and ICT as drivers of socio-economic growth is reflected in several policy frameworks and initiatives, including Vision 2030,[12] the National ICT Master Plan,[13] and the National ICT Policy. The country's population grew from over 31 million in the year 2000 to over 50 million in 2019.[14] Similarly, the Gross Domestic Product (GDP) per capita grew from USD 2,097 to USD 3,076 over the same period.[15] In 2000, Kenya ranked 206 on the Human Development Index (HDI), and 142 in 2017, marking a rise in ranking from low to medium human development. This led the World Bank in 2014 to reclassify Kenya as a lower middle-income country from a lower income country on the basis of having a gross national income (GNI) per capita of between USD 1,046 and USD 4,125.[16] However, poverty levels remain high at over 40%.

8 *Ballots to Bullets https://www.hrw.org/report/2008/03/16/ballots-bullets/organized-political-violence-and-kenyas-crisis-governance*

9 *Privacy International, Track, Capture Kill: Inside Communications Surveillance and Counterterrorism in Kenya, https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf*

10 *Alexandra Phillips Role, Revealed: Cambridge Analytica's agent in Uhuru's 2017 campaign, https://www.the-star.co.ke/news/2019-07-17-revealed-cambridge-analyticas-agent-in-uhurus-2017-campaign/*

11 *CIPESA, State of Internet Freedom in Africa, https://cipesa.org/2018/10/state-of-internet-freedom-in-africa-2018-report-focuses-on-privacy-and-data-protection/*

12 *Kenya Vision 2030 Blueprint http://vision2030.go.ke/inc/uploads/2018/05/Vision-2030-Popular-Version.pdf*

13 *Ministry of Information, Communications and Technology, National ICT Policy, http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf*

14 *The World Bank, Demographic Transition and Growth in Kenya, https://www.worldbank.org/en/news/opinion/2010/04/28/demographic-transition-growth-kenya*

15 *Institute for Economic Affairs,, Average Growth Rates during the election periods from 1992 to 2013, http://www.ieakenya.or.ke/number_of_the_week/average-growth-rates-during-electioneering-periods-from-1992-to-2013*

16 *Allan Odhiambo, World Bank confirms Kenya's lower-middle income status, https://www.businessdailyafrica.com/news/World-Bank-confirms-Kenya-lower-middle-income-status/539546-2773210-qs1wquz/index.html*

This economic growth can be attributed to infrastructure development and changes in political structures.[17] The economy is relatively liberalised and is largely driven by market demands. Connectivity has greatly improved over the last decade due to strong competition in the telecommunications industry, with ICT infrastructure development, both in rural and urban areas, being private sector led.

Although the internet is widely available, 26% of Kenyans still do not use it for various reasons, including gender disparities in access and use, affordability, and content relevance.[18] The liberalised telecommunications sector has led to the emergence of greater competition, better policies and regulations, enhanced investment in radio and TV broadcasting and ICT services, greater contribution to the economy by the ICT sector and benefits to the public including lower prices, better connectivity and access to a wide range of telecommunications products and services.

17 *African Development Bank, Kenya Economic Outlook, https://www.google.com/search?q=growth+of+kenyan+economy&oq=growth+of+kenyan+economy&aqs=chrome.0.0.8492j0j4&sourceid=chrome&ie=UTF-8*

18 *The Internet Journey for Kenya: The Interplay of Disruptive Innovation and Entrepreneurship in Fuelling Rapid Growth https://link.springer.com/chapter/10.1057/978-1-137-57878-5_2*

4 Results

4.1 Key Trends of Internet Control Over the Last Two Decades

This section traces the evolution, shifts and milestones of internet control measures in Kenya, since 1999. It provides a deeper appreciation of the intervening political and socio-economic considerations behind the different control measures as introduced and applied by different governments.

4.1.1 Weaponising the Law to Legitimise State Actions

As early as 1998, the country had introduced internet freedom infringing provisions in its ICT-related laws and policies. As ICT usage grew, the provisions became more restrictive – providing for state surveillance, interception of private communication, and online censorship, among others. Most of the legislation were introduced under the pretext of ensuring national security and fighting terrorism and cybercrime.

Legalising Surveillance and Interception of Communication

The earliest forms of surveillance in Kenya can be traced back to the colonial period.[19] The colonial government recruited mercenaries to work as guides and porters. The mercenaries later replaced the traditional leaders as chiefs. During the fight for independence, their role expanded to include surveillance on citizens who were involved in the guerrilla war. Government surveillance has continued with successive governments and has intensified during elections, following terrorism acts and global technological trends in public service administration. Twice, just before the 2017 elections, the Communications Authority announced it would set up new surveillance systems and regulatory measures.

Kenya has adopted legislation to legitimise surveillance practices through legalised interception by state agencies supported by communication intermediaries. In 1998, Kenya adopted the National Security Intelligence Service (NSIS) Act [20] which was amended in 2012 by the National Intelligence Service Act, 2012.[21] The 2012 Act establishes the NIS which is charged with gathering intelligence and regulating security intelligence in the country. Further, section 42 permits interference with persons' communications through legalised investigation. Details of the intelligence service's operations, including its budgets and operations, are classified.

19 *Following in Footsteps: The Transformation of Kenya's Intelligence Services Since the Colonial Era https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-1/pdfs/Kenya-intel-since-colonial-era.pdf*

20 *National Security Intelligence Service Act, http://kenyalaw.org/kl/fileadmin/pdfdownloads/RepealedStatutes/NationalSecurityIntelligenceService_11_of_1998_.pdf*

21 *National Intelligence Service Act, 2012 https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf*

In 2016, the communications regulator published a number of regulations related to citizen surveillance including the requirement for cybercafes to install security cameras to capture and record the identity of internet users.[22] Similarly, the Computer Misuse and Cybercrimes Act, 2018 requires communication service providers to ensure that their systems are technically capable of supporting lawful interceptions at all times, as provided by the regulatory laws in force.

Terrorism and National Security as Justifications for Repressive Laws

The protection of national security, preservation of public order, and the fight against terrorism have been used as a basis to enact repressive legislation. Moreover, these terms have not been clearly defined in the national laws and are therefore largely ambiguous and abused to extend to all aspects of society with a common trait of promoting impunity by state agencies in their operations.

Since 2008, Kenya has had frequent terror attacks from an Al-Qaeda linked Somali terrorist group, Al-Shabaab. Experts have stated that Kenya is a primary target of this group because it gives them wide international coverage.[23] Al-Shabab has carried out three major attacks in the last decade: the Westgate Shopping Centre attack in 2013, the Garissa University attack in 2015, and the most recent one, the Dusit attack, in January 2019. All these attacks have resulted in changes in surveillance and digital communications policies in the country.

In 2014, following a terrorist attack at the Westgate Shopping Mall in Nairobi in September 2013, the government introduced an amendment to the Prevention of Terrorism Act under the Security Laws (Amendment) Act, 2014.[24] The amendment limited the right to privacy under the constitution and authorised national security organs to intercept communication for the purposes of detecting, deterring, and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. The procedures are yet to be made public.

Section 43 and 44 of the Private Security Regulations Act[25] allows private security companies to search an individual and withhold their identity documents on entry to a building or any other property. The sections, however, provide some limitations to the search, such that it is done while protecting individuals' rights as provided by other laws, limits the use of identification documents only for identification purposes and only withholds the identity document to the point of the individuals' exit. Section 51(c) also prohibits private security firms from using and installing equipment that are capable of intercepting and interfering with other individuals' communication. However, this law has been poorly implemented, as there are reported cases where the security firms have advertised for services for the supply of firearms and surveillance equipment. This suggests poor cooperation between the private security firms, the government and the Private Security Authority that was established by the Act.[26]

22 *State Surveillance, Mixed Signals and Seven Years in Jail: Thoughts on Cybersecurity Regulations 2016 by Communications Authority, https://blog.cipit.org/2016/01/18/state-surveillance-mixed-signals-and-seven-years-in-jail-thoughts-on-cybersecurity-regulations-2016-by-communications-authority/*

23 *Why al-Shabaab targets Kenya and how to stop the attacks, https://qz.com/africa/1525710/nairobi-hotel-attacks-why-al-shabaab-targets-kenya/*

24 *Security Laws (Amendment) Act 2014, http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf*

25 *Private Security Regulation Act, No. 13 of 2016 http://www.kara.or.ke/Private%20Security%20Regulation%20Act%2013%20of%202016.pdf*

26 *New regulations can drive reforms in the private security sector https://www.businessdailyafrica.com/analysis/columnists/4259356-4745544-uxgipl/index.html*

Silencing Dissent and Criticism through Criminalising Free Speech

During the study period, the government has used criminal law to prosecute and punish critics. This has included the introduction of provisions in laws allegedly to tackle hate speech and fake news, and the use of arrests and intimidation of bloggers and government critics online.

Enforcing Insult Laws

In December 2014, outspoken blogger Robert Alai was arrested and charged under section 132 of the Penal Code[27] for undermining the authority of a public officer because of remarks he had made on social media concerning President Uhuru Kenyatta. He posted the statement "Insulting Raila is what Uhuru can do. He hasn't realised the value of the Presidency. Adolescent President. This seat needs Maturity" which authorities found were calculated to bring into contempt the lawful authority of the President. Alai made a constitutional challenge to the arrest and argued that the provision was vague, uncertain and an unjustifiable limitation to freedom of expression, as well as violating basic criminal law principles. In April 2017, the High Court found the provision invalid and declared that its continued enforcement was unconstitutional and a violation of the fundamental right to freedom of expression.[28]

False News/ Misinformation

The arrest and questioning of Kenyan bloggers and social media users for critical online speech has been on the rise. Since 2012, several bloggers have been arrested for critical online speech and charged over hate speech allegations. In September 2017 the National Cohesion and Integration Commission warned perpetrators of hate speech and fake news in online platforms to be ready to face the consequences.[29] The Commission cautioned that there was a need to think twice before posting any information on social media.

In May 2018, President Uhuru Kenyatta assented to the Computer Misuse and Cybercrimes Act, 2018, which introduced offences such as false publications, publication of false information, cyber harassment, and unauthorised interference and unauthorised interception. Following a petition by the Bloggers Association of Kenya (BAKE) and the Kenya Union of Journalists (KUJ), the High Court suspended the implementation of 26 provisions of the Act.[30] Those provisions impose penalties of up to ten years in prison for the publication of "false" or "fictitious" information and threaten online freedom of expression.

27 In 2017, the provision was invalidated by a High Court decision, https://www.article19.org/resources/kenya-win-for-freedom-of-expression-as-penal-provision-declared-unconstitutional/

28 Robert Alai v The Hon Attorney General & another [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/135467/

29 NCIC Warns Hate Speech And Fake News Perpetrators Ahead Of Petition Ruling, https://www.capitalfm.co.ke/news/2017/09/ncic-warns-hate-speech-fake-news-perpetrators-ahead-petition-ruling/

30 Petition 206, http://kenyalaw.org/caselaw/cases/view/159286

Criminal Defamation

Criminal defamation laws have been used against government critics. The Kenya Information and Communication Act, 2009[31] under the now repealed section 29,[32] made it an offence to send, through a licensed telecommunication system, a message that is grossly offensive or of an indecent, obscene or menacing character; or to send a message that one knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person. The offence carried a penalty of KES 50,000 (USD 500) or three months imprisonment, or both. Several bloggers and journalists were threatened, arrested and detained over this offence.[33] In the period between January 2015 and April 2016, 32 bloggers had been arrested and charged under this provision.[34] However, the charges were dropped once the High Court declared the provision unconstitutional in May 2016.

In addition, section 194 of the Penal Code[35] also provided for criminal defamation and was used to target those criticising government or other individuals. It provided that "Any person who, by print, writing, painting or effigy, or by any means otherwise than solely by gestures, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, is guilty of the misdemeanour termed libel". Two people were arrested and charged under the section for defaming a prominent lawyer by publishing a post about him on a social media platform that handles consumer protection complaints. The two brought a constitutional petition challenging the charges, and the High Court in February 2017 declared the provision unconstitutional as it was a violation of freedom of expression.[36] The charges were subsequently dropped.

Excessive and Punitive Responses

In August 2012, Robert Alai was arrested and charged under section 29 of the Kenya information and Communication Act, over a tweet alleging that the then government spokesperson, Alfred Mutua, had ordered the execution of G.P. Oula and Oscar King'ara, and that the spokesperson wanted to kill him too.[37] In a separate tweet, the outspoken blogger called the spokesperson a "foolish pig". The charges were later dropped.

31 *Kenya Information and Communication Act http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/KenyaInformationandCommunicationsAct(No2of1998).pdf*

32 *Why Justice Mumbi Ngugi declared Section 29 of KICA Unconstitutional, https://www.ifree.co.ke/2016/05/justice-mumbi-ngugi-declared-section-29-kica-unconstitutional/*

33 *96 Bake Condemns The Arrest And Intimidation Of Kenyans Online, https://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/*

34 *, Bloggers and Journalists relieved after law on "misuse of communication devices" declared unconstitutional, http://www.talkafrica.co.ke/bloggers-and-journalists-relieved-after-law-on-misuse-of-communication-devices-declared-unconstitutional/*

35 *Penal Code https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/28595/115477/F-857725769/KEN28595.pdf*

36 *Jacqueline Okuta & another v Attorney General & 2 others [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/130781/*

37 *Blogger's arrest shines light on Kenya's internet freedoms, https://itweb.africa/content/o1Jr5qxE32xvKdWL*

In 2013, the government enacted the Media Council Act[38] which provided for the establishment of the Media Council with the mandate to put in place media standards and to ensure compliance with those standards as outlined in Article 34(5) of the Constitution. There was an outcry from the media fraternity when the Media Council Bill[39] was being enacted on the grounds that the law was intended to muzzle free speech and to curtail the freedom of the media which is protected by the Constitution of Kenya. The Media Council Act was viewed as a weapon to regulate bloggers, journalists and other social media users in Kenya through the Media Council. The Act imposed a statutory code of conduct while the Kenya Information and Communications (Amendment) Act[40] drew criticism for undermining self-regulation through the government appointment Tribunal, thus undermining self-regulation and therefore having a chilling effect on press freedom.[41]

In 2013, the government introduced amendments to the Kenya Information and Communication Act to establish a Multimedia Appeals Tribunal, which could impose fines of up to KES 20 million shillings (USD 20,000) if a person is found culpable under the law. While media bodies lodged a court case arguing that these two laws were oppressive and unlawful,[42] and in May 2016, the High Court found the laws to be constitutional.[43]

In August 2017, blogger Robert Alai was arrested and forced to remove content from his Facebook platform.[44] The blogger had posted photos of members of President Kenyatta's family mourning the death of a family member at a Nairobi hospital.

In June 2019, Alai was arrested again, detained for 14 days, and forced to delete content that he had posted on his Facebook page. He was charged with disclosure of information in relation to terrorist activities, under Section 19 of the Prevention of Terrorism Act, 2012. The content related to photos of police officers who had been killed in a terrorist attack in Wajir County.[45] The government officials condemned the action which they termed "irresponsible" and accused the blogger of "glorifying terrorism". Alai responded that the post was justified as he was speaking for deprived police officers who had been neglected, and their allowances had been taken by "wakubwa" (senior people).

On both incidents, Kenyans quickly took to social media demanding Alai's release with the hashtag #FreeAlai in support of the once fierce government critic. This was the first time a blogger was being charged under the anti-terrorism law. The use of such legal provisions can create a powerful instrument that enables authorities to control journalistic activities and free expression online.

38 *Media Council Act, 2013 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2046%20of%202013*

39 *Media Council Bill, 2013 http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2013/THEMEDIACOUNCILBILL.pdf*

40 *Kenya Information and Communication (Amendment) Act http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2013/KenyaInformationandCommunications_Amendment_Act2013.pdf*

41 *Wanyama, L., Media Control in Kenya: The State of Broadcasting under the New Kenya Information and Communication Act of 2013, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.679.8285&rep=rep1&type=pdf*

42 *Media bodies move to court to challenge new law, https://www.nation.co.ke/news/Media-moves-to-court-to-challenge-new-law/1056-2156004-mhm6p6z/index.html*

43 *Blow to media as court declares 'draconian laws' constitutional, https://www.the-star.co.ke/news/2016-05-27-blow-to-media-as-court-declares-draconian-laws-constitutional/*

44 *Why Statehouse Operative Ordered CID Police to Arrest Blogger Robert Alai, https://www.kenya-today.com/politics/statehouse-operative-ordered-cid-police-arrest-blogger-robert-alai-arrested*

45 *Blogger Robert Alai arrested for posting gory photos, https://www.capitalfm.co.ke/news/2019/06/blogger-robert-alai-arrested-for-posting-gory-photos/*

4.1.2 Disrupting Communication Networks

Following the 2007 post-election violence,[46] the government blamed communications mediums such as broadcast media and SMS for fanning the violence.[47] It banned live broadcasting prior to the announcement of election results, citing "public safety and tranquillity", prompting citizens to turn to SMS and social media to circumvent the televised media blackout. The government also disabled bulk SMS to prevent people from sending "provocative messages" or "hate speech".[48] The government thereafter established the National Cohesion and Integrated Commission (NCIC) in 2008 to aid in fighting online and offline hate speech.[49]

Kenya has not experienced any major internet shutdown but media blocks have been experienced over the years. Ahead of the general election in August 2017, there were fears that there would be an internet shutdown. However, the Communications Authority (CA) confirmed that it had no such intentions. While it attributed this to the fact that Kenya is a mature democracy, other observers opined that it may have been a result of government wishing to benefit from the spread of false content and fake news which were motivating more people to go to the polls, hence the political cost for shutting down the internet may have been too high.[50] The CA and the NCIC published guidelines dealing with transmission of bulk SMS and social media for public consultation. According to the CA, the guidelines applied to "collaborative arrangements with other stakeholders such as bloggers, Social Media Services Providers, among others". The CA cited its power to issue the guidelines under Section 23 and 25 of the Kenya Information and Communications Act (KICA), 1998.

In January 2018, Kenyans woke up to a shutdown of all major media channels including KTN News, Citizen TV and NTV on all their platforms following the swearing in of opposition leader Raila Odinga on January 30, 2018.[51] The government had threatened an instant shutdown of any media house that would live stream the event. The shutdown contravened Article 33 of the Constitution which states that broadcasting and other electronic media have freedom of establishment, subject only to licensing procedures that are necessary to regulate the airwaves and other forms of signal distribution. The TV stations were to be shut down for 14 days before the High Court suspended the shutdown.[52]

4.1.3 Surveillance Galore: The Build-Up of the State's Capacity

Despite the existence of several provisions within the legal and policy frameworks, surveillance and interception of communication in the country has been on the rise since 2000. The government has continued to enhance its technical capacity to intercept and conduct surveillance in line with approaches in other countries such as the USA, Russia and China.

46 The violence resulted in the death of 1,133 people and the displacement of over 300,000 people.

47 https://repository.upenn.edu/cgi/viewcontent.cgi?article=1012&context=ictafrica

48 Social Media and Post-Election Crisis in Kenya, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1012&context=ictafrica

49 Footprints of peace, https://www.cohesion.or.ke/images/docs/FOOTPRINTS-OF-NCIC.compressed.pdf

50 Mutung'u, G., Did Fake News Save Kenya from an Internet Shutdown? Emerging Trends in Tech and Elections in Africa, Berkman Klein Centre for Internet and Society at Harvard University, https://cyber.harvard.edu/events/2017/10/Mutungu

51 Nyabola, N., Putting Kenya's Media Shutdown into context, https://www.aljazeera.com/indepth/opinion/putting-kenya-media-shutdown-context-180202092850790.html

52 Kenya Court suspends government media shutdown, https://www.aljazeera.com/news/2018/02/kenya-court-suspends-government-media-shutdown-180201143724641.html

Going High-Tech to Implement Surveillance

Buoyed by an enabling legal framework, the government has taken steps to enhance its technical capacity for surveillance and interception of communications through the installation of hardware and software with capacity for surveillance and working with communication service providers to monitor and intercept private communications.

In March 2012, Kenya's telecommunications regulator wrote to internet service providers seeking their cooperation in the installation of the Network Early Warning System (NEWS) tool in order to detect cyber threats and respond to cyber incidents by monitoring network traffic[53] and to promote cybersecurity.[54] The NEWS tool was capable of monitoring traffic and needed to interface with the ISP networks to collect data on the networks' incoming and outgoing traffic and their speeds. A section of the operators opposed the move, stating that it would expose them to legal suits. It is not clear whether the operators ultimately complied with the requirement and whether the system is in place.[55]

In June 2014, the government awarded Safaricom, the largest mobile phone services provider, a tender to set up a communications and security surveillance system at a cost of 14.9 billion shillings (USD 4.9 million). The CCTV system, installed at public spaces and along key roads, was procured from the Chinese company Huawei. The system directly links to all security agencies and to a central command centre.[56] The controversial system was installed in the absence of a data privacy law, heightening fears among the general public of the country turning into a police state.

However, six years later, the cameras are unreliable as they are not functional and cannot be relied on for security purposes.[57] Further, the Auditor General noted that there is poor coordination between the National and county government on their maintenance.[58] Meanwhile, these installations were done without policies and guidelines on how data would be collected and used. Article 31 of the constitution ensures the right to citizens' privacy yet oftentimes, the footage has been leaked to the public via social media, infringing individuals' right to privacy.

In 2016, the military was reported to have bought a KES 1 billion (USD 10 million) drone to aid in the fights against the Al Shabab.[59] The drone was expected to enable the collection of real time data on the terrorist hideouts, training, recruitment activities and communications.

There are no adequate checks and balances on the design, deployment and use of digital surveillance technologies that are currently in use. While surveillance is permitted in national legislation, the risk is that the practice can go unchecked as the technologies become more sophisticated, hard to detect and widespread. Further, it may be difficult to hold the government or the companies that develop and sell such systems accountable, owing to the secretive nature of their operations and their covert systems that continue to make it difficult to even establish their existence in telecommunications networks.

53 *CCK to spy on Internet users, https://www.nation.co.ke/news/CCK-to-spy-on-Internet-users-/1056-1370842-dux0xd/index.html*

54 *Mark, O., CCK to spy on internet users, https://www.nation.co.ke/news/CCK-to-spy-on-Internet-users-/1056-1370842-dux0xd/index.html*

55 *Freedom House, Freedom on the Net 2013 - Kenya, https://www.refworld.org/docid/52663ae85.html*

56 *Safaricom reveals Huawei involvement in CCTV tender, https://www.standardmedia.co.ke/article/2000125287/safaricom-reveals-huawei-involvement-in-cctv-tender*

57 *Most CCTV security cameras in Nairobi unreliable, https://www.businessdailyafrica.com/news/Most-CCTV-security-cameras-in-Nairobi-unreliable/539546-4967638-njy6nn/index.html*

58 *Thiong'o, J, Why Kshs 437 Million CCTV Cameras in Nairobi are not working, millions of lives at stake, https://www.standardmedia.co.ke/business/article/2001312225/why-sh437-million-cctv-cameras-in-nairobi-are-not-working*

59 *Otuki, N., Kenya buys 1bn pilotless aircraft in war on Al Shabaab, https://www.businessdailyafrica.com/economy/Kenya-buys-Sh1bn-pilotless-aircraft-in-war-on-Al-Shabaab/3946234-3091184-6lsmy3z/index.html*

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

Measures have been introduced progressively in the country to enable the government identify telecommunication services users with precision. From SIM card registration, the government has sought to introduce new programmes to enable digital identities that incorporate biometrics with poor or no oversight.

SIM Card Registration

Kenya introduced SIM card registration in 2015, requiring all mobile network providers under rule 4 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 to register all SIM card subscribers.[60] Failure to provide the information as per SIM card regulations is an offence punishable by a fine of KES 300,000 (USD 3,000) or to imprisonment for a term not exceeding six months, or both. Mandatory SIM card registration requires users to provide their names, photo ID, telephone and email contacts, postal and physical addresses.

Rapid Adoption of Biometric Data Collection

Following Kenya's disputed 2007 presidential elections, the country's election management body, the Independent Electoral and Boundaries Commission (IEBC), introduced Biometric Voter Registration (BVR), an electronic voter identification and a biometric voter register. The system captures the data of voters including their photo, fingerprints and other personal identification information.

As more businesses digitalise their services and operations, the government has also sought to digitalise public services as it seeks to benefit from the public's openness to using new technologies and platforms. The first major digitalisation program was the e-citizen initiative introduced in 2012 as a one-stop platform for multiple government services such as passport application and business registration services. Consequently, more services, such as registration of drivers' licences, were included. The e-citizen is supplemented by Huduma Centres, dubbed as one-stop service centres using post offices countrywide for multiple public services such as ID application, business registration and National Hospital Insurance Fund (NHIF) registration.

In September 2017, Kenya launched an East African Community e-Passport that contains the holder's biometric information on a tamper-proof page, to curb fraud and ease clearance at immigration. The move followed a directive from the 35th EAC Council of Ministers meeting in April 2017 for member states to issue e-passports by January 2018. In the same year, the government introduced the National Education Management Information System (NEMIS)[61] which assigns students from the age of five years a Unique Personal Identifier (UPI) that provides real-time data that guides the management and allocation of resources to public schools.

60 Regulations, https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf

61 Ministry of Education, , NEMIS, http://nemis.education.go.ke/

Other data collection systems include iTax, an online tax filing system; the Integrated Customs Management System (iCMS), for real-time monitoring of goods entering the country through the Mombasa port and airports; and the Electronic Cargo Tracking System (ECTS) for transit cargo. The government also operates the Integrated Financial Management Information System (IFMIS).

Similarly, in January 2019 President Kenyatta announced the development of a central master population database, known as the National Integrated Identity Management Systems (NIIMS), which would be the authentic 'Single source of truth' on personal identity in Kenya.[62] The database is expected to replace the integrated Population Registration System (IPRS), and contain information on all Kenyan citizens as well as foreign nationals residing in Kenya. For each registration, the system will generate a unique identification number known as Huduma Namba.[63] The mass registration process was conducted in May 2019, and captured the details of 37.7 million people.[64]

The digitalisation of services, however, has locked out those who are unable to go online whether due to costs or digital illiteracy, thus making accessing these services more elusive as well as more expensive. Applications for tax returns and driving licences through e-citizen have promoted the use of intermediaries (people who can assist others to apply for these services at a fee).

4.1.5 Enter the Era of Social Media and Data Taxation

One of the notable and concerning phenomena of the more recent years is the use of taxation to undermine citizens' use of the internet. In some instances, such measures have been designed partly as a clear measure to limit how many citizens can access digital technologies and use them to hold governments to account. In other instances, governments have been eager to increase revenues from the telecom sector. In the last two years, enhancing taxes on airtime, data bundles and social media access appears to be evolving as a pattern. These costs are usually passed on to consumers, thereby raising the cost of owning and using a mobile phone and the internet.

In July 2018, Kenya's Finance Act 2018[65] increased the excise tax on telephone airtime from 10% to 15%, and introduced a 15% excise tax on internet data services and fixed line telephone services.[66] The increases, which were passed on to consumers,[67] were seen as regressive in nature and construed by consumers as the government's intention to discourage the use of mobile phone services. Kenya first introduced a tax on mobile phone airtime in 2003 via an excise tax rate of 10% and 16% Value-Added Tax (VAT) on mobile handsets.[68]

62 *The Digital Identity Ecosystem, https://www.nimc.gov.ng/digital-identity-ecosystem/*

63 *Speech by Uhuru Kenyatta, http://www.president.go.ke/2019/01/22/speech-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-during-a-meeting-with-senior-security-officials-at-state-house-mo/*

64 *Huduma Namba, http://www.hudumanamba.go.ke/; Another Huduma Namba listing planned for those who missed out, https://www.the-star.co.ke/news/2019-07-06-government-plans-for-another-huduma-namba-listing/*

65 *Finance Act, 2018 https://www.kra.go.ke/images/publications/Finance-Act-2018.pdf*

66 *Taxing mobile transactions, https://www.brookings.edu/wp-content/uploads/2019/08/Taxing_mobile_transactions_20190806.pdf*

67 *Safaricom increases voice, SMS and data prices to reflect 15pc Excise Duty, https://www.capitalfm.co.ke/business/2018/10/safaricom-increases-voice-sms-and-data-prices-to-reflect-15pc-excise-duty/*

68 *Taxing mobile phone transactions in Africa: Lessons from Kenya https://www.brookings.edu/research/taxing-mobile-phone-transactions-in-africa-lessons-from-kenya/*

4.1.6 Deploying Bots, Cyberattacks and Disinformation

A common excuse for curtailing internet freedom is the need to fight what the government terms misinformation, disinformation, hate speech, or fake news, among other terms.

Yet the government itself has at times sought to control discussions on social media through its propaganda machinery. In the run-up to the 2017 general election, the government recruited key online influencers such as Robert Alai, who was hitherto a fierce critic of the government, to support government narratives online. Further, it is said to have recruited 36 bloggers and sourced social media bots to drive government propaganda and influence conversations online.[69]

Further, the ruling Jubilee party had during the same period hired embattled firm, Cambridge Analytica, a political-data analysis firm, to support its campaigns during the August 2017 election.[70] The company is reported to have rebranded Uhuru Kenyatta's party, written its manifesto, done two rounds of surveys each involving 50,000 respondents, and developed its messaging including writing speeches.[71] The firm distributed misinformation, sponsored advertisement through Facebook and other online platforms on the possibilities of violence breaking out if the strongest rival to Kenyatta won the election. Although it is not known whether Cambridge Analytica influenced the outcome of elections, it possibly contributed to the hostile online environment during the election period. The government also raided the opposition's offices and deport its data science workforce before the team even commenced its work.[72]

69 *Uhuru regime hires 36 bloggers as online war with opposition rages, https://www.kenya-today.com/news/government-hires-36-bloggers-as-online-war-with-opposition-rages*

70 *Revealed: Cambridge Analytica's agent in Uhuru's 2017 campaign, https://www.the-star.co.ke/news/2019-07-17-revealed-cambridge-analyticas-agent-in-uhurus-2017-campaign/*

71 *Cambridge Analytica: How potential propaganda filled the minds of Kenyan voters, https://www.standardmedia.co.ke/ktnnews/video/2000151852/cambridge-analytica-how-potential-propaganda-filled-the-minds-of-kenyan-voters*

72 *Why The Government Raided And Deported NASA's Foreign Campaign Strategists, ttps://kenyainsights.com/why-the-government-raided-and-deported-nasas-foreign-campaign-strategists/*

4.2 Key Positive Developments

Despite the negative trends witnessed in Kenya, there were notable developments that were indeed positive and that support the enjoyment of internet freedom. The three major developments included the robust advocacy and push-back by non-state actors, the adoption of progressive legislation and lastly, the repeal of repressive legislation.

4.2.1 Advocacy and Push-back by Non-State Actors

In 2006, the United Nations Secretary General announced the establishment of the Internet Governance Forum (IGF) and in 2008, Kenya convened its first ever national IGF. The IGF presented a multi-stakeholder platform to discuss public policy issues related to internet governance. Currently the annual Kenya IGF convened for the past decade by the Kenya ICT Action Network (KICTANet) has transformed from being a multi-stakeholder platform to a forum that presents opportunities and safe spaces for Kenyans to meet and directly engage with government policymakers.

In July 2017, civil society organisations criticised the imposition of guidelines by the Communication Authority and the NCIC on bulk SMS transmission and social media. According to the Authority, the guidelines applied to "collaborative arrangements with other stakeholders such as bloggers, social media services providers, among others." The CA cited its power to issue the guidelines under Section 23 and 25 of the Kenya Information and Communications Act (KICA), 1998. The human rights organisation Article 19 stated that the CA was acting outside the scope of its powers in issuing the guidelines, which it purported to apply to bloggers and social media services providers.[73] Others argued that the guidelines were tantamount to censorship[74] as they restricted the right of bloggers and ordinary Kenyans to use the internet.

In May 2018, the Bloggers Association of Kenya (BAKE) challenged several problematic provisions of the Computer Misuse and Cybercrimes Act, 2018[75] which contained offences relating to fake news, investigative procedures and cyber harassment. According to BAKE, the law did not meet the constitutional threshold of laws. It argued that the new law was an attempt to reintroduce criminal defamation laws, which had previously been declared unconstitutional. The High Court suspended the coming into force of 27 provisions of the Act, pending the determination of the case.[76]

73 *New Draft Guidelines on dissemination via Electronic Communications Networks should be scrapped, https://www.article19.org/resources/kenya-new-draft-guidelines-on-dissemination-via-electronic-communications-networks-should-be-scrapped/*

74 *Kenya: This Is Internet Censorship Through the Back Door, https://allafrica.com/stories/201707060473.html*

75 *Computer Misuse and Cybercrimes Act http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf*

76 *Justice Chacha Mwita Suspends 26 Sections Of The Computer Misuse And Cybercrimes Act, https://www.blog.bake.co.ke/2018/05/29/justice-chacha-mwita-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act/*

In another case, the Kenya Human Rights Commission[77] challenged the constitutionality of the National Integrated Identity Management System (NIIMS) based on the use of a miscellaneous amendments law[78] to introduce substantive amendments, the lack of public participation in the process, inadequate frameworks to guarantee data privacy and protection, and the risk that the system could further entrench discrimination and exclusion of marginalised groups in Kenya. In April 2019, the High Court issued interim orders restricting the government while they carried out the Huduma Namba enrolment exercise.[79] Until the full case concluded, the government was restricted from making Huduma Namba registration mandatory, linking Huduma Namba to public services, collecting DNA or GPS, setting any deadline for registration, or sharing the data collected with third parties.

4.2.2 Adoption of Progressive Legislation

Kenya has adopted some laws and policies with progressive provisions since the year 2000, which have provided greater protection for human rights. In 2016, Kenya adopted the Access to Information Act.[80] although it is yet to be fully implemented and at the same time, the Official Secrets Act[81] remains in force.

In 2006, the government released the Information and Communications Technology Sector Policy Guidelines (ICT Policy).[82] This policy was anchored on internationally accepted standards and best practices, particularly pertinent to the Common Market for Eastern and Southern Africa (COMESA) Model as was ratified and adopted by the COMESA Council of Ministers in March 2003.[83] The main aim of this policy was to facilitate sustained economic growth and poverty reduction, promote social justice and equity, mainstream gender in national development, empower the youth and disadvantaged groups, stimulate investment and innovation in ICT and achieve universal access. It has specific policy objectives on information technology, broadcasting, telecommunications, and postal services, among others.

Meanwhile, the Constitution of Kenya, 2010[84] expanded the Bill of Rights particularly in the areas of non-discrimination, the provision of checks and balances, devolution, separation of powers, media freedoms and freedom of thought. In relation to media freedoms, articles 31, 33, 34, 35 and 36 promote the rights to privacy, freedom of expression, media freedoms, the right to information and freedom of assembly and association respectively. The Constitution also established independent oversight institutions, and all laws have been subjected to review to align them to the constitution.

77 *NIIMS is legally flawed, offers no protection against cybercrime https://www.standardmedia.co.ke/article/2001312597/niims-is-legally-flawed-offers-no-protection-against-cyber-crime*

78 *Statute Law (Miscellaneous Amendments) Act, 2018 http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf*

79 *Huduma Namba stopped! https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/704-press-release-huduma-namba-stopped.html*

80 *Access to Information Act, 2016 https://www.cuk.ac.ke/wp-content/uploads/2018/04/Access-to-Information-ActNo31.pdf*

81 *Official Secrets Act https://www.nis.go.ke/downloads/Official%20Secrets%20Act,Cap%20187.pdf*

82 *ICT Policy https://www.researchictafrica.net/countries/kenya/National_ICT_Policy_2006.pdf*

83 *Report and Decisions: 17th Meeting of the COMESA Council of Ministers Report, 4-5 June 2004, Nile International Conference Centre, Kampala, Uganda http://www.iri.edu.ar/publicaciones_iri/anuario/CD%20Anuario%202005/Africa/38-comesa_ministers-17th%20meeting.pdf*

84 *Constitution of Kenya, 2010 http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010*

4.2.3 Repeal of Repressive Legislation

In Kenya, constitutional challenges at the High Court spearheaded by civil society have over the past five years led to successes in repealing or suspending unconstitutional legislation. In April 2016, Justice Mumbi Ngugi declared that section 29 of the Kenya Information and Communications Act (KICA) on the offence of “misuse of a licensed telecommunication system” was unconstitutional.[85] Further, Justice Ngugi ruled that the provision was too broad and hence impossible for one to ascertain how not to contravene it. She stated, "If the intention was to protect the reputation of others, then there are clear provisions in the law of libel." The section had been used to penalise bloggers and social media users for using ICT to disseminate messages that were deemed “grossly offensive” or to cause “annoyance, inconvenience or needless anxiety to another person”. The prescribed a fine was KES 50,000 (USD 500) or a three-month jail term for anyone found guilty of the offence. The Court ruling[86] was welcomed by civil society organisations that championed free speech in Kenya, as the provision was an affront on civil liberties and prone to abuse by authorities keen to clamp down on free speech.

Criminal defamation as provided for under Section 194 of the Penal Code was declared unconstitutional following a case at the High Court in February 2017.[87] In his ruling, Justice Mativo stated that criminal libel was an unjustifiable limitation of freedom of expression, that the prospect of criminal proceedings and a jail term of up to two years for defamation was

85 Law on Misuse of communication devices declared illegal, https://www.standardmedia.co.ke/article/2000198855/law-on-misuse-of-telecommunication-devices-declared-illegal

86 Petition No. 149 of 2015 Judgment, Retrieved from: https://www.article19.org/data/files/medialibrary/38343/Judgment-Petition-No.-149-of-2015-2-1.pdf

87 Jacqueline Okuta & another v Attorney General & 2 others [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/130781/

88 Robert Alai v The Hon Attorney General & another [2017] eKLR, http://kenyalaw.org/caselaw/cases/view/135467/

5 Conclusion and Recommendations

5.1 Conclusions

Kenya has since 2000 gained significantly from the liberalisation of its telecommunications sector and will continue to benefit from competition in the sector. The report found the use of big data, censorship and surveillance as emerging areas of concern. Further, political insecurity, whether election-related or terrorism-related, adversely affect internet freedom given the government's disproportionate measures to address them. The increased adoption of digitalisation globally, has also brought about pressure to adopt such developments at the national level, albeit without data protection frameworks in place.

Other factors that need to be monitored include elections, state capture, democracy, good governance, technological development, political activism and the roles of independent oversight institutions such as the Judiciary and Parliament. These factors have been key in appreciating the role of the state in ensuring internet freedom.

While certain state measures have been repressive with time, the public has shown resilience in the face of repressive laws, censorship, surveillance and even big data initiatives. In some instances, the government has conceded its wrong-doing. However, the role of the courts has been instrumental as a defender of internet freedom given the level of judicial activism in recent public interest litigation cases. Sadly, arrests, detention and intimidation of bloggers and journalists continue and will need to be monitored and challenged to check state excesses. Therefore, there is still more work to be done by all relevant actors to safeguard the space for the enjoyment of internet freedom in Kenya.

54 *Jimmy Kainja (August 2019) Are Malawians Sleepwalking Into a Surveillance State? https://bit.ly/3056e6y accessed 8th January 2020*

5.2 Recommendations

The study makes the following recommendations targeting government, companies, civil society, media, technical community, and academia.

The government should:

- Promote affordable access to the internet and internet-enabled devices.
- Promote public trust in public institutions by following court orders.
- Continue to bridge the digital divide through measures to enhance connectivity, accessibility and affordability of the internet. .
- Provide assistance for access by the public to e-government services though the Huduma Centres.
- Enact the Data Protection Bill in line with international standards on data protection and privacy.
- Amend laws in line with the Constitution and implement them in the spirit of the Constitution.
- Develop the capacity of law enforcement officers and the Judiciary in handling cases that relate to emerging Internet Governance issues.

Companies should:

- Adhere to laws and policies relating to internet freedoms.
- Comply with the United Nations Business and Human Rights principles to ensure the rights of their customers are protected.
- Adopt best practices and principles of privacy and data protection such as the GDPR including promoting privacy by design, and developing and adhering to privacy policies.
- Engage policy makers to ensure regulation promotes human rights principles.
- Invest in internet infrastructure to bridge the digital divide.

The media should:

- Advocate for the independence of the media.
- Establish in-house policies for the protection of their journalists.
- Promote transparency in their ownership.
- Conduct journalism in accordance with the code of ethics.
- Promote digital security training for journalists.

Academia should:

- Promote evidence-based policy decision making through research.
- Effectively communicate research to policy stakeholders.
- Engage with other stakeholders to promote online freedom.

The technical community should:

- Develop innovation that improves society including enabling access to the internet for marginalised groups such as persons with disabilities, women and the elderly.
- Promote the protection of internet freedom online.

Civil Society should:

- Continue to advocate for the promotion and protection of internet freedom.
- Continue to represent in court persons whose internet freedom has been infringed.
- Build capacity for government, the tech community and private sector actors on internet freedom.
- Enhance digital security for human rights defenders.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org