Navigating Kenya's Digital Information Ecosystem

Funded by
the European Union

Internews
Local voices. Global change.

Navigating Kenya's Digital Information Ecosystem

By Chaacha Mwita[1], Anne Mikia, and David Odongo

Funded by
the European Union

Internews
Local voices. Global change.

[1] Lead Researcher

About

KenSafeSpace

Kenya Safe and Inclusive Digital Space (KenSafeSpace) is a European Commission funded multistakeholder project, aimed at strengthening the voice, capacity, and influence of Kenyan human rights organisations, to promote and safeguard democratic, safe, and inclusive digital space. Internews together with its partners KICTANet, Internet Without Borders, Mzalendo Watch, Bloggers Association of Kenya (BAKE), Tribeless Youth and Watoto Watch Network, will support Human Rights Civil Society Organisations (HR CSOs), media professionals, and individuals, to be able to accurately identify, monitor, and respond to online disinformation, hate speech, cyberbullying, and other digital risks, through delivering a combination of targeted research, tailored training and tools, and innovative human-centered and rights-based solutions.

Internews

Internews, is an international media development organization which empowers local media worldwide, and which has been in operation since 1982. With international headquarters in Washington DC and Africa headquarters in Nairobi, Internews works to ensure access to trusted, quality information that empowers people to have a voice in their future and to live healthy, secure, and rewarding lives.

Disclaimer

This publication was funded by the European Union. Its contents are the sole responsibility of the author and do not necessarily reflect the views of the European Union.

Funded by the European Union

Foreword

Established in Kenya since 2004, Internews has supported partners around the world to demand, build and protect a safe, accessible internet for more than two decades, with a particular focus on the world's most vulnerable populations. From funding local internet rights advocacy to designing cutting-edge security, we connect our local and regional partners globally and provide technological support to media outlets and human rights defenders. Our Global Tech Hub equips individuals and organisations with the tools and knowledge they need to defend themselves against targeted attacks, so they can operate safely in an increasingly dangerous online environment.

Kenya's digital media landscape is exponentially growing with internet penetration at 40.08 percent and over 13 million social media users. Majority of those who are connected are relying on more than one platform for their media consumption habits, which include, communicating, socializing, receiving information or news. Recently social media platforms have played a significant role in organizing, mobilising and coordinating participation in demonstrations. However, this boom is synonymous with the rise of disinformation, hate speech and other various cyber threats that have detrimental effect to vulnerable groups of people like the marginalised and underserved communities, children, women and young people who may not have the skills and tools to protect themselves from online threats.

To effectively understand the digital status, gaps and intricate use of social media in Kenya, we commissioned Mr. Chaacha Mwita and his team of researchers, who have analysed the digital information ecosystem and published very useful insights and recommendations. This assessment addresses amongst others, the need to safeguard data online, countering harmful content by empowering journalists and content creators to verify and counter disinformation, promoting digital media literacy and cyber hygiene practises amongst vulnerable groups, building robust cyber security infrastructure and policies that foster innovation, mitigate insecurity and do not curtail human rights. The report calls for social media platforms to remain accountable and against inauthentic use of artificial intelligence.

Abraham Mariita
Project Director, KenSafeSpace - Internews

Contents

Acronyms and Abbreviations

AI	Artificial Intelligence
BAKE	Bloggers Association of Kenya
CA	Communication Authority
DCI	Directorate of Criminal Investigations
DIEA	Digital Information Ecosystem Assessment
FGD	Focus Group Discussion
ICT	Information and Communication Technology
IHUB	Innovation Hub
INGO	International Non-Governmental Organisation
KICTANet	Kenya ICT Action Network
KII	Key Informant Interview
KOT	Kenyans on Twitter
KRA	Kenya Revenue Authority
KUJ	Kenya Union of Journalists
MCK	Media Council of Kenya
NGO	Non-Governmental Organisation
OGBV	Online gender-based violence
PWD	Person with disability
USF	Universal Access Service Fund

Executive Summary

This digital information ecosystem assessment (DIEA) in Kenya represents an effort to understand the digital threats and risks in relation to digital media and AI, key human rights issues that may be affected or exacerbated by harmful[2] online speech, digital policy gaps and readiness in Kenya. It aims to yield recommendations that would make the digital environment in Kenya safe for everyone. Through a qualitative study, integrating current secondary quantitative data, the DIEA endeavours to unravel key issues and perspectives that define Kenya's digital safety.

The findings are sobering: Firstly, Kenya faces a staggering number of digital threats every day! With 1.3 billion cyberthreats detected in just the second quarter of the 2023/2024 financial year[3] , the country experiences more than 1.4 million cyberthreats per day or 1,000 per second.

Secondly, Kenya has a highly engaged online population, particularly the youth, who are active participants in online platforms like X (formerly Twitter) but with a definite gender skew… males dominate this space by far. This online population, loosely coalescing around the acronym KOT (Kenyans on Twitter) and mostly made up of Gen-Z, has led effective digital activism and offline action as well. However, they operate in a digital terrain fraught with dangers.

In mapping digital sources of information, several key groups emerged from the FGDs. Social media platforms (Facebook, TikTok, X and others) are all the rave for their accessibility, agility, and breaking news ability. Online news websites like Citizen Digital, Nation, and Star are considered reliable by many due to their credibility, depth, and accessibility, although challenges such as paywalls, clickbait headlines, and biased reporting were noted. Blogs and niche websites offer specialised content and foster community engagement yet concerns about their credibility and adherence to journalistic standards were raised. Email and messaging apps, particularly WhatsApp and Telegram, facilitate rapid communication and information sharing but face issues with spamming and misinformation, leading to user concerns about privacy and information overload. Lastly, Artificial Intelligence (AI) is viewed as both a tool and a source of information.[4] While AI applications like ChatGPT and Grammarly enhance productivity and creativity, concerns about algorithmic bias, authenticity (easily manipulable to abuse others), and addiction to it were highlighted. Need for curated content and parental controls to mitigate AI-related issues was observed, underscoring the importance of balancing AI use with genuine human experiences.

Further, this research found that the country has impressive indices such as internet penetration (40.8 percent[5]), digital innovation and entrepreneurship, mobile money and financial inclusion, and government digital initiatives. Yet a plethora of digital threats are identifiable. They include cyber threats (such as phishing), social threats (such as online harmful speech including mis/disinformation and online gender-based violence [OGBV]), financial threats (such as fraud), identity theft threats (such as impersonation), AI-related risks (such as manipulability for abuse), and regulatory risks (such as gaps in data protection laws).

In addition, this research shows low media literacy and lack of critical thinking skills, especially among vulnerable groups of digital information users more so the elderly, children, and Persons with Disabilities (PWDs) of all ages and socio-economic status. It also shows that education and journalism have been most impacted by digitisation and are serious battlegrounds in the fight against digital threats affecting freedom of expression and personal agency rights.

Further, telecommunication companies stand accused of poor service levels regarding connectivity, pricing, poor refund policies, and neglect of certain demographics, especially PWDs. This is despite the fact that Kenya's digital terrain is regulated broadly, with more than 20 laws being applicable to digital operations.

A significant number of Kenyans express helplessness and defencelessness in the face of a digital onslaught — pervasive threats, information overload, mis and disinformation, and bewildering AI and the implications it portends in different spheres (job security, human rights, exacerbating the digital divide and so on).

[2] See Figure 3

[3] CA (2024), 'Second Quarter Sector Statistics Report Financial Year 2023/2024'; https://repository.ca.go.ke/bitstream/handle/123456789/1369/Sector%20Statistics%20Report%20Q2%202023-2024.pdf?sequence=1&isAllowed=y — accessed on Monday June 24, 2024 at 10:15am

[4] For instance, in response to the question "Where do you get your information from and why?", many FGD participants mentioned ChatGPT. A student from a local university who participated in the Nakuru FGD said her colleagues don't even "bother to read books; they go straight to ChatGPT".

[5] Data Reportal (2024), 'The State of Digital in Kenya'; https://datareportal.com/reports/digital-2024-kenya

There are obvious gaps such a weak cybersecurity framework, a legal terrain that is neither robust nor up to date, to effectively prosecute modern forms of digital misconduct, and lack of capacity within the law enforcement cadres.

From the insights gathered, a series of recommendations emerge to bolster digital safety across various stakeholders. For KenSafeSpace, having commissioned this foundational study, they can directly utilise these findings to enhance programme impact and scalability. Key recommendations for the project include training journalists and content creators in ethical standards, enhancing digital media literacy, and promoting responsible content dissemination practices to uphold authenticity and mitigate misinformation risks, overaly contributing to online safety. In addition, KenSafeSpace should consider working with policy research and engagement organisations to influence policy in the digital environment and collaborating with Government and civil society organisations in public awareness campaigns about digital security and responsible online behaviour.

Recommendations for the Government of Kenya include engaging youth in internet governance, promoting digital literacy in education, reforming educational curricula to include digital skills, and establishing ethical AI guidelines. Furthermore, creating a dedicated entity to combat cybercrime, regulating digital practices with foresight, and bridging the digital divide are crucial steps towards a secure digital environment that protects individual rights and fosters inclusive digital participation.

Civil society should conduct public awareness campaigns, community support initiatives, and lobbying for robust regulatory frameworks to safeguard digital rights and enhance safety online. Meanwhile, donors can facilitate collaboration among stakeholders, supporting initiatives that enhance collective defence capabilities and promote inclusive digital safety measures globally.

The private sector, custodians of vast public data repositories, should invest in secure technologies, and empower users, especially vulnerable groups, to control their digital experiences and protect their rights. Lastly, individuals and corporations alike should invest in robust cybersecurity measures, stay informed about digital threats, and responsibly manage their online presence to contribute to a safer digital ecosystem for all.

In conclusion, digital threats exist and safeguarding the integrity of the digital space requires collaborative efforts from stakeholders across sectors. Collective efforts are essential in mitigating cyber risks and fostering a secure digital environment conducive to innovation and global connectivity.

> *“Kenya has a highly engaged online population, particularly the youth, who are active participants in online platforms like X (formerly Twitter) but with a definite gender skew… males dominate this space by far.*

Landscape Overview

Due to rapid technological developments, the digital landscape in Kenya has become an integral part of everyday life, shaping how information is produced, disseminated, and consumed. The entry of AI has complicated the terrain somewhat. On one hand there are immediate benefits to these developments; on the other, there's an explosion of new threats and risks that require mitigation for better safety online and enjoyment of human rights generally.

This DIEA, carried out in the Kenyan context, seeks to identify digital threats and risks, awareness of them by the general population, policy gaps in addressing these threats and risks and make recommendations for different stakeholders — the project that commissioned the report, government agencies, the civil society, individuals and the private sector.

Kenya's digital landscape is enabled by the National ICT Policy,[6] which outlines aspirations and strategies for steering the country's information and communication technology sector. The policy emphasises expanding and upgrading ICT infrastructure to ensure broadband internet, mobile networks, and related technologies are accessible nationwide, aiming to bridge the digital divide and reach rural and marginalised communities.

Central to the policy is the theme of digital inclusion, striving to provide equal opportunities for all citizens to access and benefit from ICT services. This extends to government operations, with initiatives enhancing public service delivery through digital platforms and citizen engagement tools.

Innovation and entrepreneurship are also key focal points, with efforts by government through the Kenya Digital Blueprint[7] directed towards creating a conducive environment for tech start-ups and fostering creativity within the ICT sector. Education plays a vital role, with plans[8] to integrate ICT into the curriculum to equip students with necessary skills, while cybersecurity measures are prioritised to safeguard against digital threats and ensure secure ICT use.

Kenya's digital information landscape is a vibrant tapestry woven by a multitude of stakeholders, each contributing to the production, distribution, and consumption of digital information in distinct yet interconnected ways. At the heart of this landscape lie diverse sources of information — media platforms ranging from traditional outlets like newspapers, television, and radio (most of which have a digital presence of their legacy versions) to the dynamic digital media platforms encompassing blogs, social media platforms, and online news portals.

Traditional media, including newspapers, television stations, and radio broadcasters, have long been central to Kenya's information landscape. Despite facing challenges such as declining circulation and financial strain[9], these entities continue to play a significant role in shaping public discourse, including on digital threats and risks, creating awareness on these, and advocating policy options.

Kenya's telecommunications sector plays a central role in keeping the digital ecosystem engine running. The country boasts a robust telecommunications infrastructure, including extensive mobile and fixed-line networks. Mobile penetration is particularly high (110 percent)[10] , with multiple providers offering competitive services. Safaricom, Airtel, and Telkom Kenya are the leading mobile operators, offering voice, data, and mobile money services. Safaricom's M-pesa mobile money platform is especially notable for its widespread adoption and impact on financial inclusion.

Kenya has witnessed significant growth in internet penetration, driven by the widespread adoption of mobile technology. According to the CA, smart phone penetration is at almost 67 percent of the population[11] , while

6. Ministry of Information, Communications and Technology, Kenya (2019), National Information, Communications and

7. Technology (ICT) Policy; https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf - accessed on Monday June 24, 2024 at 10:51 am.

ICTA (2022), Kenya National Digital Masterplan 2022: https://cms.icta.go.ke/sites/default/files/2022-04/Kenya%20Digital%20Masterplan%202022-2032%20Online%20Version.pdf

8. Ministry of Information, Communication and Technology, Kenya (2019)

9. Mwita, C (2021), The Kenya Media Assessment 2021, Internews, Nairobi; https://internews.org/wp-content/uploads/legacy/2021-03/KMAReport_Final_20210325.pdf - accessed on Monday June 24, 2024 at 10:25 am.

10. CA (2024)

broadband subscription in the country is at 73 percent[12]. With a youthful population and very high smartphone penetration, access to the internet has become more available (and utilised) across urban and rural areas. Mobile internet usage, facilitated by different data plans and expanding 4G coverage, has transformed how Kenyans access information, communicate, and engage with online services. And the demand for these services continues to rise. According to Londa 2023: Digital Rights and Inclusion in Africa Report: "In 2023, … local demand for internet grew in Kenya by 19.6 percent to 9.6 million Gigabytes per second (Gbps) compared to 8.1 million Gigabytes per second (Gbps) in 2022."[13]

These factors — significant internet penetration, prevalence of smart phones, youthfulness of the population, rising demand for digital services etc. — have propelled the use of social media as a source of information and tool for information sharing to almost quarter of the country's population[14], an unprecedented high so much as to emerge the leading source of news and information in Kenya in some studies.[15]

Kenya's digital landscape is characterised by a dynamic ecosystem of start-ups, tech hubs, and innovation centres, fostering creativity and entrepreneurship. Nairobi, often referred to as "Silicon Savannah,"[16] serves as a hub for tech innovation, attracting local and international investors, developers, and entrepreneurs. From fintech and e-commerce to agritech and healthtech, Kenyan start-ups are leveraging digital technologies to address local challenges and create scalable solutions for global markets. These include initiatives like Farmer Lifeline Technologies[17] , Innovation Hub (iHub)[18] and the Kenya ICT Action Network (KICTANet) Think Tank[19].

Somehow related to the foregoing point on digital innovation and entrepreneurship, is the impact of mobile money and financial inclusion through digitisation in Kenya. No discourse on the digital space in Kenya can conclude without this key highlight. Kenya has gained international recognition for its pioneering mobile money service, M-pesa, which has revolutionised financial inclusion and digital payments.[20] M-pesa's widespread adoption has transformed how Kenyans conduct financial transactions, access credit, and manage their finances, particularly among unbanked and underbanked populations. The success of mobile money has spurred innovation in digital finance and fintech, contributing to Kenya's position as a leader in financial inclusion with some studies showing that approximately 90 percent of Kenya's adult population has access to financial services.[21] Unfortunately, this success has opened the floodgates of financial fraud as we shall see.

The Kenyan government has prioritised digital transformation as a key driver of economic growth and development as seen from the National ICT Policy. Various initiatives, such as the Digital Literacy Programme, Huduma Centres, eCitizen platform, and the Universal Access Services Fund (USF)[22] , aim to expand technology reach, harness it to improve service delivery, enhance transparency, and promote citizen engagement. Additionally, the establishment of institutions like the Communications Authority of Kenya (CA) and the Kenya Information and Communications Technology Authority (ICT Authority) underscores the government's plans to advancing ICT infrastructure and policies.

The (USF) in particular, could have far-reaching consequences in terms of internet accessibility for all. A government initiative established to promote universal access to ICT services across the country, particularly in underserved and remote areas, USF aims to bridge the digital divide by ensuring that all Kenyan citizens, regardless of their location or socio-economic status, have access to affordable and reliable ICT infrastructure and services. The key objective of the fund is digital inclusion through infrastructure development, affordability, capacity building, and partnerships. Through its initiatives and investments, the fund aims to create a more connected, informed, and empowered society where everyone can benefit from the opportunities offered by ICT.

[11] CA (2024)

[12] CA (2024)

[13] Paradigm Initiative (2024), Londa: A Digital Rights and Inclusion in Africa Report 2023, Lagos, Nigeria: https://paradigmhq.org/londa-23/

[14] Data Reportal (2024)

[15] Mwita (2021)

[16] Ubuntu Life (2022), Welcome to the Silicon Savannah: How Kenya is becoming the next Global Tech Hub; https://www.ubuntu.life/blogs/news/welcome-to-the-silicon-savannah-how-kenya-is-becoming-the-next-global-tech-hub - accessed on Monday June 24, 2024 at 11:05am.

[17] https://farmerlifeline.co.ke

[18] https://ihub.co.ke

[19] https://www.kictanet.or.ke

[20] Capmad (undated), Financial Inclusion in Kenya: The M-pesa Success Story
https://www.capmad.com/technology-en/financial-inclusion-in-kenya-the-m-pesa-success-story/#:~:text=The%20company%20plays%20a%20critical,2%20%25%2C%20or%20250%2C000%20people — accessed on Monday June 24, 2024, at 11:10 am.
Capmad (undated)

[21] CA (2023); https://www.ca.go.ke/universal-access-overview

In the context of digital information production, distribution, and consumption, regulatory bodies such as the CA and MCK play pivotal roles. These entities are responsible for overseeing various sectors, including telecommunications, broadcasting, and online publishing. They regulate these domains to ensure adherence to standards, fair competition, and safeguard the interests of both consumers and industry stakeholders. Through their oversight, the CA and MCK contribute to maintaining the integrity and reliability of Kenya's digital information ecosystem.

Other key stakeholders that actively shape the direction and vitality of the digital ecosystem in Kenya include prominent media associations, civil society organisations, and international entities. Organisations such as the Kenya Union of Journalists (KUJ), the Bloggers Association of Kenya (BAKE), and the KICTANet Think Tank, alongside international non-governmental organisations (INGOs) like Internews, assume pivotal roles encompassing media monitoring, advocacy, training, and research initiatives. Through their collective efforts, these groups contribute significantly to the overall health and vibrancy of Kenya's digital information environment, fostering a culture of accountability, innovation, and inclusivity.

And lastly there are audiences or consumers who are the primary targets of content and services offered or facilitated by various entities. They are integral stakeholders in the digital media ecosystem, actively contributing to its dynamics, sustainability, ethical and security considerations through their consumption, feedback, and advocacy.

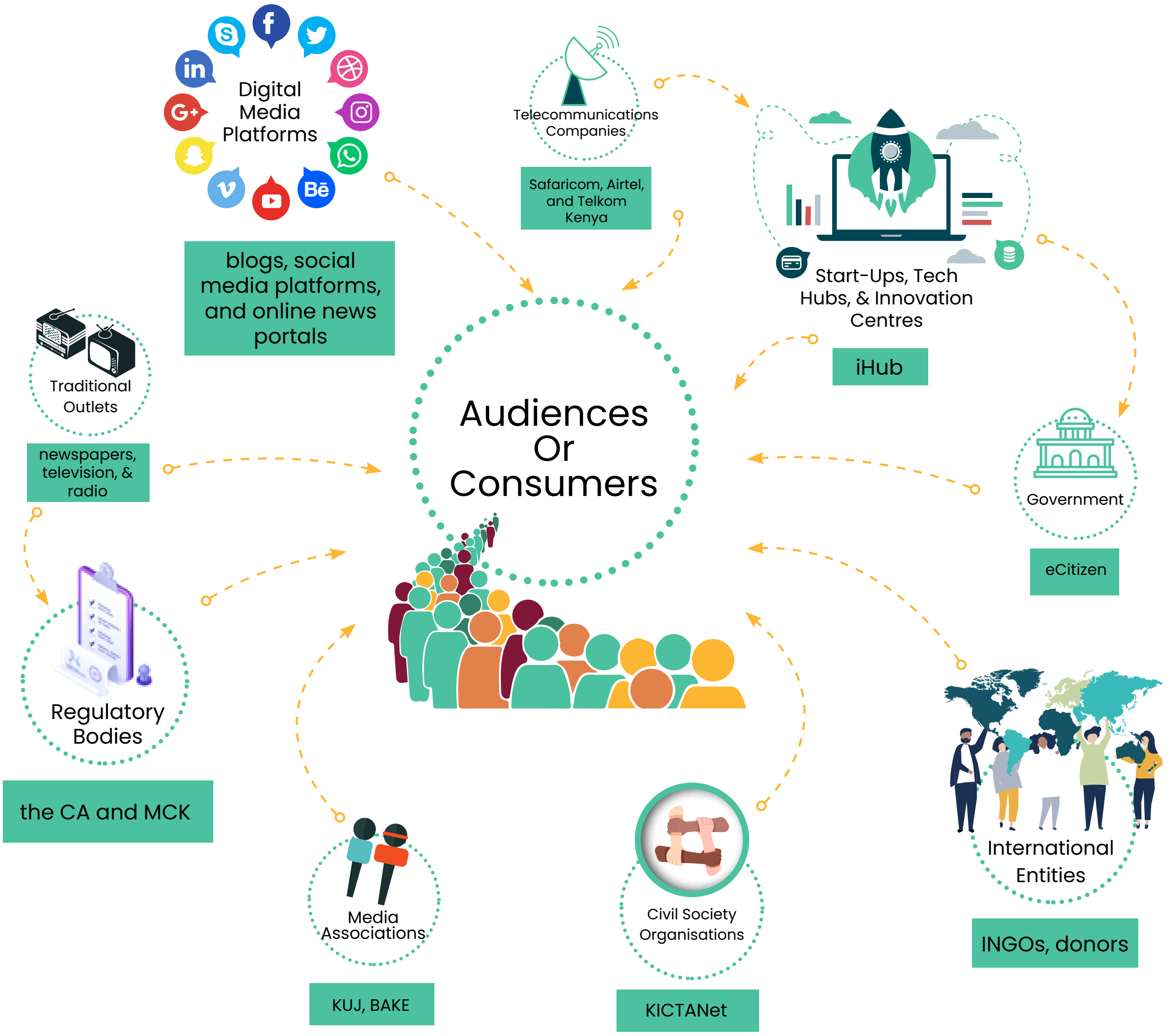

Digital Media Platforms
blogs, social media platforms, and online news portals
Telecommunications Companies
Safaricom, Airtel, and Telkom Kenya
Start-Ups, Tech Hubs, & Innovation Centres
iHub
Traditional Outlets
newspapers, television, & radio
Audiences Or Consumers
Government
eCitizen
Regulatory Bodies
the CA and MCK
Media Associations
KUJ, BAKE
Civil Society Organisations
KICTANet
International Entities
INGOs, donors

Figure 1: Illustration of stakeholder in the digital media ecosystem.

By way of concluding this introduction, scope and landscape overview section, the scope of this DIEA is limited to the identification and analysis of digital risks and threats in the Kenyan context, awareness of them by the general population, policy gaps in addressing these threats and risks and recommendations for different stakeholders to make Kenya a more digitally safe environment. Integral to this process is the mapping and analysing digital sources of information in the country.

The assessment lays emphasis on how despite advanced infrastructure, many laws, progressive plans and pronouncements, and so on, digital threats still exist and adversely affect the general population, often disproportionately like, marginalised and vulnerable groups such as children, youth, PWDs, the elderly, and indigenous peoples. Moreover, the assessment aims to gauge public awareness, concerns, and political attitudes towards digital threats, providing a crucial barometer of societal sentiment.

> *...despite advanced infrastructure, many laws, progressive plans and pronouncements, and so on, digital threats still exist and adversely affect the general population, often disproportionately like, marginalised and vulnerable groups such as children, youth, PWDs, the elderly, and indigenous peoples.*

Findings and Analysis

1. Kenya's digital space is threatened by cyberattacks, harmful speech and other online threats

Key findings from the literature review, the key informant interviews (KIIs) and focus group discussions (FGDs) is that Kenya is a digitally insecure environment. According to the latest statistics from the CA, there were 1.3 billion cyberthreats detected in just the second quarter of the 2023/2024 financial year, marking a staggering 943 percent increase from 124 million in the previous quarter.[23] That averages out to 1.4 million threats per day. During the same quarter, the CA report says, 8.1 million cyberthreat advisories were issued for Kenya, a 44.4 percent rise from the previous quarter's 5.6 million.[24]

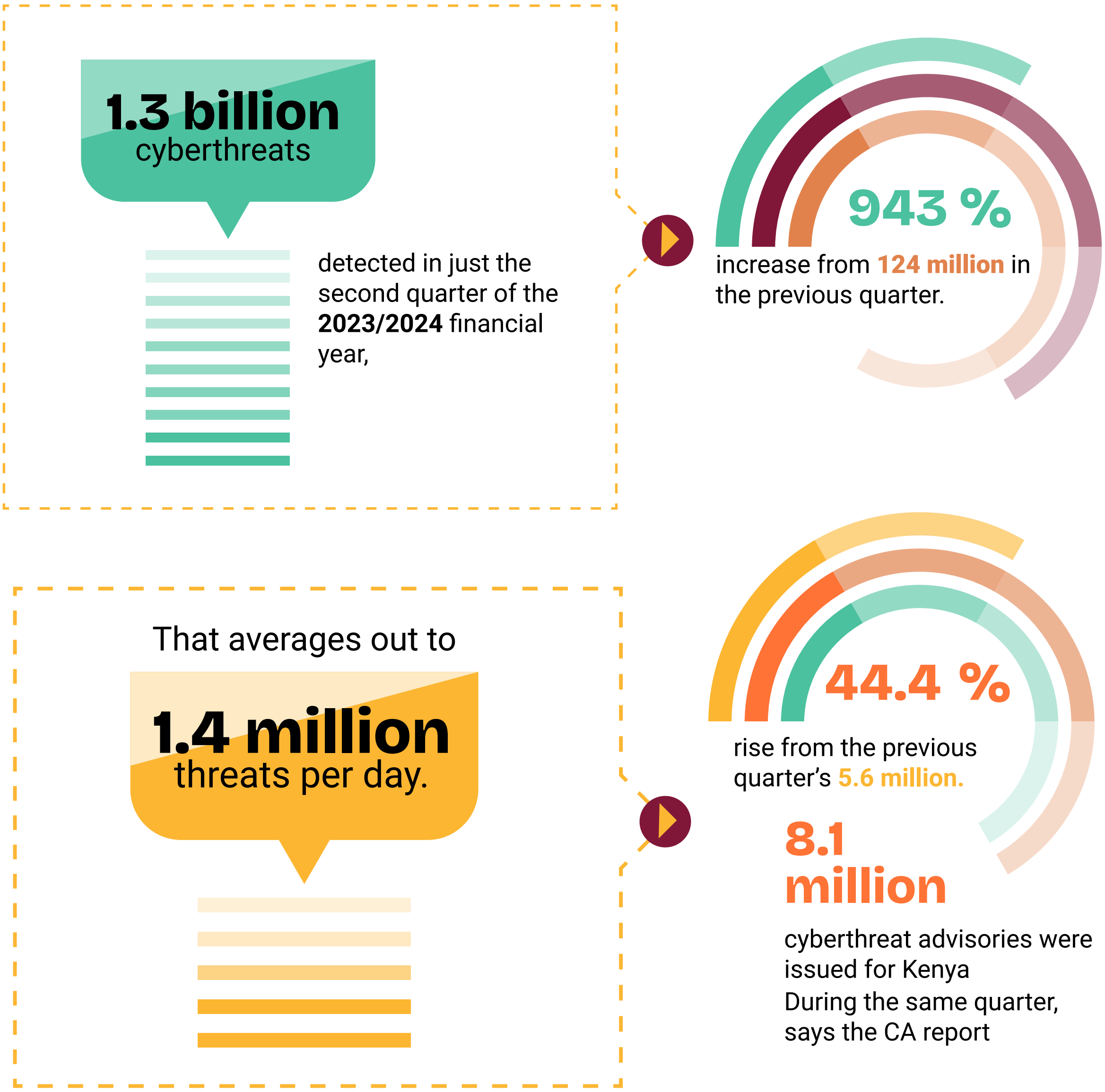
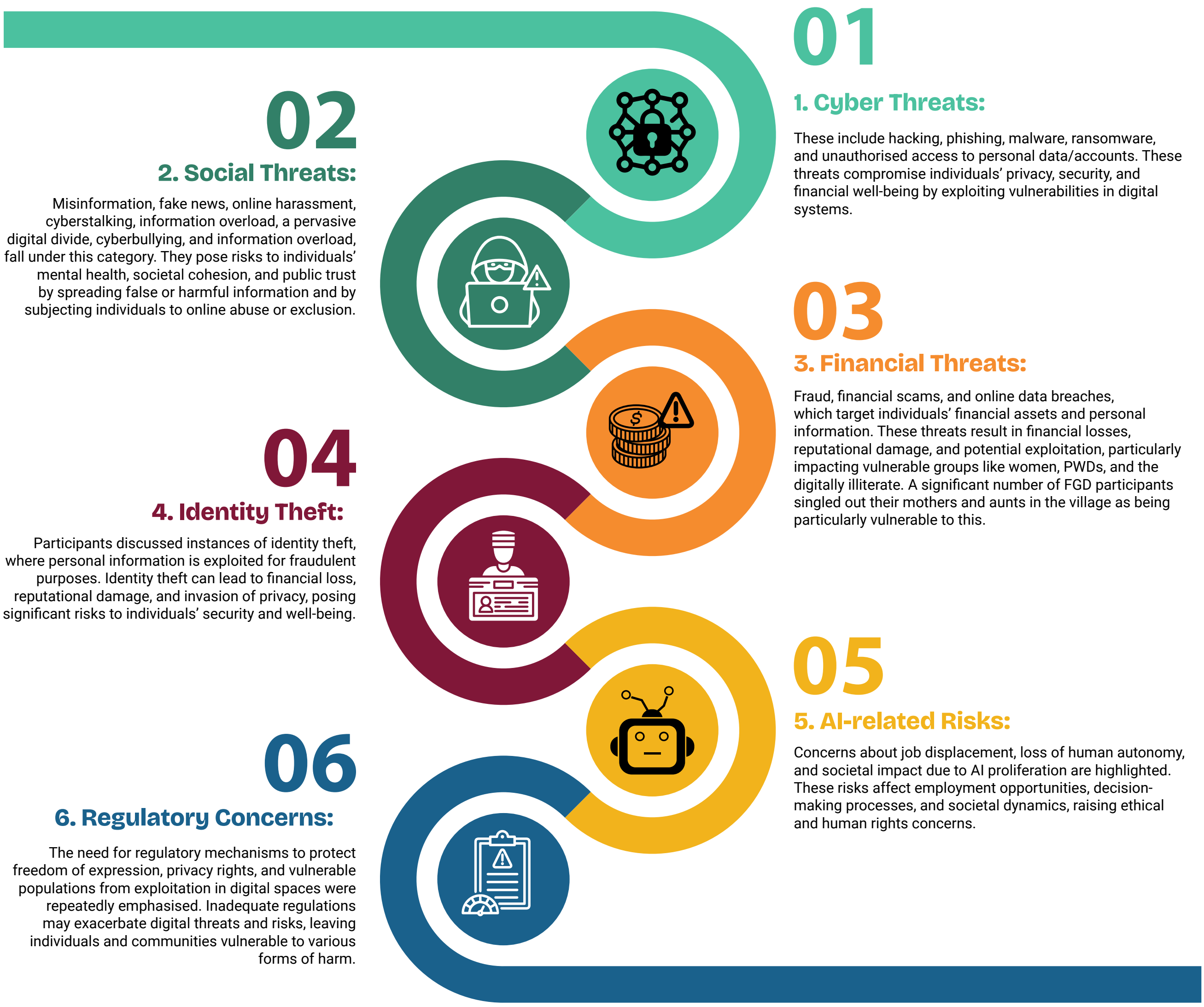


Figure 2: Graphic illustration of digital threats in Kenya. Source - CA.

[23] CA (2024)
[24] CA (2024)

This digital insecurity is reflected in testimonies from various participants, some of which are cited herein below. From the FGDs and KIIs, Kenyans encounter an array of threats and risks that have the potential to compromise their privacy, security, and well-being. There were at least six groups of digital threats identified and least 25 individual digital threats and risks explicitly mentioned during the FGDs and KIIs as analysed below.



01

1. Cyber Threats:

These include hacking, phishing, malware, ransomware, and unauthorised access to personal data/accounts. These threats compromise individuals' privacy, security, and financial well-being by exploiting vulnerabilities in digital systems.

02

2. Social Threats:

Misinformation, fake news, online harassment, cyberstalking, information overload, a pervasive digital divide, cyberbullying, and information overload, fall under this category. They pose risks to individuals' mental health, societal cohesion, and public trust by spreading false or harmful information and by subjecting individuals to online abuse or exclusion.

03

3. Financial Threats:

Fraud, financial scams, and online data breaches, which target individuals' financial assets and personal information. These threats result in financial losses, reputational damage, and potential exploitation, particularly impacting vulnerable groups like women, PWDs, and the digitally illiterate. A significant number of FGD participants singled out their mothers and aunts in the village as being particularly vulnerable to this.

04

4. Identity Theft:

Participants discussed instances of identity theft, where personal information is exploited for fraudulent purposes. Identity theft can lead to financial loss, reputational damage, and invasion of privacy, posing significant risks to individuals' security and well-being.

05

5. AI-related Risks:

Concerns about job displacement, loss of human autonomy, and societal impact due to AI proliferation are highlighted. These risks affect employment opportunities, decision-making processes, and societal dynamics, raising ethical and human rights concerns.

06

6. Regulatory Concerns:

The need for regulatory mechanisms to protect freedom of expression, privacy rights, and vulnerable populations from exploitation in digital spaces were repeatedly emphasised. Inadequate regulations may exacerbate digital threats and risks, leaving individuals and communities vulnerable to various forms of harm.

Figure 3: Illustration of groups of digital threats

a. Hacking:

This is the unauthorised access to personal accounts, leading to loss of control over personal information and potential dissemination of sensitive content without consent. During the FGDs, there were many account hacking narratives shared. For instance, a young discussant from Eldoret shared how his Facebook account was hacked, and pornography posted in it. He only learnt about it when friends started asking him what he was sharing. It took him a lot of effort and time to delete the content, but the damage had already been done. He said he was left with a dented image among friends and relatives.

b. Phishing:

These are deceptive attempts to obtain sensitive information, such as login credentials or financial details, posing risks of identity theft and financial fraud. A discussant from Kisumu believes her Facebook account was hacked after successful phishing, underscoring the importance of not sharing login credentials with anyone, “not even relatives”, she said. After her Facebook account was hacked, the hacker asked for money in exchange for the account. She decided to abandon the account and open a new one.

c. Mis/disinformation:

This refers to fabricated or sensationalised news stories, contributing to misinformation and potentially causing confusion, division, and harm to individuals and communities. This is rampant in Kenya, especially around election time,[25] with internationally notorious purveyors of mis/disinformation such as Cambridge Analytica having been implicated at least once — in the 2017 elections. FGD participants highlighted the challenge of distinguishing between credible information and misinformation or fake news, emphasising the importance of fact-checking and verifying sources.

d. Online harassment:

These are persistent and unwelcome behaviour online, including cyberbullying and cyberstalking, causing emotional distress, mental health issues, and reputational damage. This affects women disproportionately, accounting for a significant part of OGBV globally[26] . A lady discussant in Kisumu shared how she was stalked on and through Facebook until she started avoiding official functions. The stalker would give detailed information on her, her dressing, her social life, and even associations. She reported this to Facebook, but no action was taken. She experienced six months of stalking until she blocked everybody and started a new list of friends. She said she’s now more knowledgeable on how to keep safe online by not posting personal information and data including photos.

e. Financial fraud:

This involves deceptive schemes aimed at defrauding individuals or organisations of financial assets, leading to monetary losses and reputational damage. A banker from Nairobi, narrated how he was scammed (and “parted with a significant amount of money”) by con artists who subsequently told him on phone, “you can’t get your money back; you’ve been conned”.

f. Data and Identity theft:

This refers to unauthorised access to personal or sensitive data, compromising individuals’ privacy, security, and potentially leading to identity theft or financial exploitation. A speech-impaired (Deaf) discussant from Nairobi, narrated how, duty to his disability he is forced to use other people for most of his digital transactions, and how one such person once gave his information to a scammer thinking he was helping.

g. Scamming:

These are deceptive schemes aimed at tricking individuals into providing personal information or financial assets, leading to monetary losses and potential identity theft. A PWD discussant in Kisumu shared how she was called by scammers posing as bank officials and asked for her personal details which she innocently shared. These were used to steal money from her phone and bank account. In addition, the scammers used her credentials to borrow money from a [mobile money loan app] and [the bank’s] M-pesa-linked loan service. She was slow in learning of all of this and, therefore, in reporting it to the police, the bank and the telecommunication company, which gave the thieves ample time to continue stealing in her name and from her. But even after she reported, action was not fast enough and so the loses continued. Her story emphasises the real-world consequences of digital threats such as account hacking and data theft.

[25] Lilian Olivia, L. (2023); ‘Disinformation was rife in Kenya’s 2022 election’, LSE - https://blogs.lse.ac.uk/africaatlse/2023/01/05/disinformation-was-rife-in-kenyas-2022-election/#:~:text=In%202022%2C%20the%20number%20of,disseminated%20on%20TikTok%20and%20Twitter.

[26] Galal, A. (Undated); Harmful Speech Watch: A Social Media Monitoring Methodology, Internews

h. Unethical use of AI:

Unethical use of AI can manifest in several ways that harm individuals or societies. Such can include privacy violations due to unwarranted surveillance or unauthorised data collection, discrimination and bias such as biased algorithms (in hiring, in provision of information, and in limited access for marginalised groups), deception and misinformation (in creating realistic fake content like deepfakes or spread of false information to manipulate opinions), and in creating and deploying autonomous weapons leveraging AI to make lethal decisions without human oversight. The AI threat was discussed at length in all FGDs. While direct discourse on AI was emotive and bewildering for some, its pervasive influence remained palpable. Participants discern the subtle manipulations wielded by AI-powered algorithms, shaping digital experiences and perpetuating phenomena like filter bubbles and misinformation cascades. The ethical dilemmas arising from AI's ascendancy, particularly concerning privacy and access to accurate information, underscored the imperative for rigorous examination within the sphere of digital rights.

Other acknowledged threats include malware (malicious software designed to infiltrate, damage, or gain unauthorised access to computer systems, potentially leading to data theft, financial loss, or system disruption); ransomware (malicious software that encrypts data and demands payment for its release, posing risks of financial loss, data breaches, and disruption to operations); and impersonation (pretending to be someone else online for fraudulent purposes, such as scamming, spreading false information, or damaging someone's reputation).

Moreover, harmful[27] online behaviour, such as addiction, and speech such as deep fakes, radicalisation, hate speech, discrimination, and social engineering were of great concern to participants due to their capacity to upset social harmony. Participants and KIIs also dwelt quite a bit on online child abuse, OGBV, and online blackmail and extortion as threats that face vulnerable groups. Other threats mentioned are body shaming, illegal betting, exclusion (widening the digital divide), and sextortion

How Harmful is Harmful?

Category	Colour	Title	Description	Word Examples
Physical	⚫	6-Death	Literal threats of kiling a person or group	Kill, annihilate, extinct, destroy, murder, massacre, eliminate, assassinate etc.
	🔴	5- Physical Violence	Threats of physical harm	Hurt,rape, toture, beat, injure, harm, wound, burn etc.
Psychological	🟠	4- Demonishing/ Dehumanising	Describing or insulting individuals/ groups with sub-human language	Cockroach, vermin, rats, alliens, nazis,monsters, monkeys, germs etc
	🟡	3-Negative Character	Non-violent insults(including vulgar insults)	Stupid, crazy, idiot, f**ker,w**ker, fool etc.
Difference	⚪	2- Negative Actions	Hopes for non-violent action	May they be defeated, they must be stopped etc.
	🟢	1- Disagreement	General disagreement, attempts to persuade or change someone's mind	False, wrong, incorrect, disagree etc.

Figure 4: How harmful is harmful? Source: Galal, A. (Undated)

[27] See Figure 3 below.

Overall, these threats affect certain demographics more than others. Children were flagged as being particularly vulnerable online, with cyberbullying and online grooming posing significant risks globally, including in Kenya. According to a KII conversant with children's rights online, these issues often involve coercion into sexual acts or exploitation through digital platforms. Sextortion, she said, where boys are blackmailed after sharing sexual images, and AI-generated sexual content featuring minors on the dark web further exacerbate these concerns. Despite existing legislation such as the Computer Misuse and Cybercrime Act and the Children's Act, there is a critical need for laws specifically addressing AI-related threats to children, another KII from Nairobi said.

The children's rights KII noted that while the DCI Child Protection Unit is instrumental in managing online safety cases, bureaucratic obstacles hindered direct communication. She also observed that telecommunication companies have a limited role in addressing these issues, though some collaborations with civil society exist. A key challenge identified is parental awareness and involvement; many parents lack understanding of digital risks and how to manage them effectively.

A mother's perspective further emphasised the importance of active parental supervision and open communication in managing children's online activities. She noted the sacrifices made for internet access and advocated for better network stability and government guidance on social media use to secure children's safety. The interview underscored the collective responsibility of parents and the government in creating comprehensive strategies to safeguard children online, stressing the need for collaborative efforts to ensure a safer digital environment for young users.

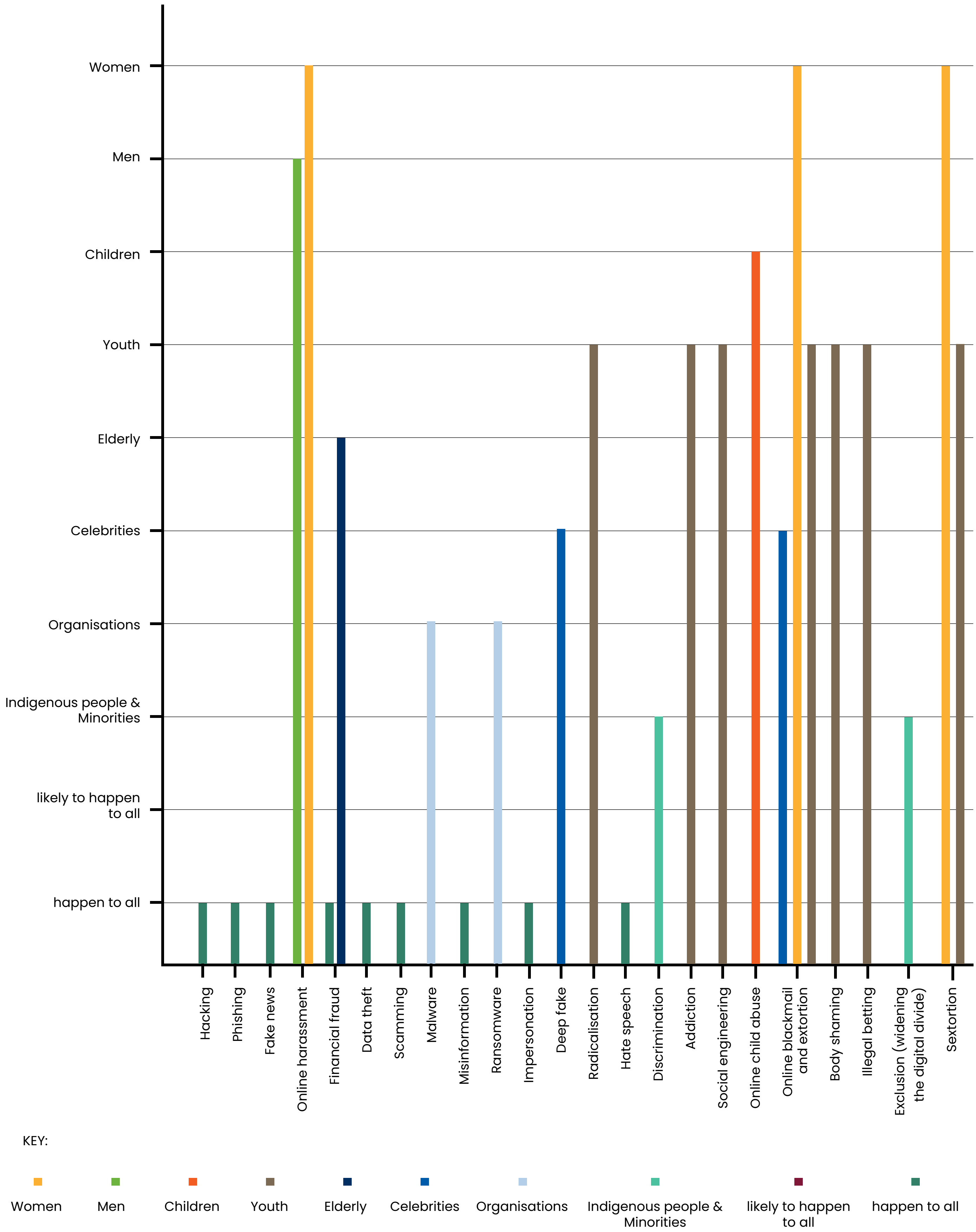
Another group whose vulnerability online was emphasised is women. This is reflected in the comic book Women and Data: Keeping Safe Online[28] , published by KICTANet Think Tank. It teaches women how to protect themselves online and combat OGBV. The comic illustrates the story of Amani, an aspiring presidential candidate whose personal data, gathered from a government registration, is misused to create AI-generated pornography that damages her reputation. She suffers from severe online and offline harassment, which leads her to withdraw from social media for her mental well-being. A KII from Nairobi says the book's narrative is not farfetched and stresses the importance of understanding the implications of one's online actions and the necessity for improved training and awareness. OGBV includes various harmful behaviours such as harassment, cyberstalking, threats, revenge porn, doxing, and coercion. These actions can occur across numerous online platforms and are often widespread and relentless. Victims may face severe psychological distress, reputational damage, social isolation, and in extreme cases, physical harm or suicide, the KII says.

As our sampling included indigenous people, youth, children, women, PWDs, and men — in between were members of the professional ranks, corporate types, and NGO workers — below is a table/figure/graphic representing how these threats may disproportionately affect certain groups more than others.

OGBV includes various harmful behaviours such as harassment, cyberstalking, threats, revenge porn, doxing, and coercion. These actions can occur across numerous online platforms and are often widespread and relentless. Victims may face severe psychological distress, reputational damage, social isolation, and in extreme cases, physical harm or suicide, the KII says.

[28] KICTANet (2022); Women and Data: Keeping Safe Online; https://www.kictanet.or.ke/comic-on-women-data-keeping-safe-online/

Threats by Demography



These individual threats and risks collectively highlight the diverse challenges posed by digital advancements and the need for comprehensive strategies to mitigate their impact on individuals, communities, and societies. Instructively, that these threats came up in FGDs, and yet actually constitute the entire spectrum of digital threats and risks, proves that a significant number of Kenyans are aware of prevalent digital threats and risks.

2. An active online population with a gendered skew

The second significant finding is that Kenya has a highly engaged online population, particularly the youth, who are active participants in online platforms like X (formerly Twitter) … but with males dominating this space by far[29] . Kenya stands out globally as the home of "Kenyans on Twitter" (KOT), a loose group to which every Kenyan on Twitter is assumed to belong. KOT has noteworthy influence on policy, and now has the capacity for physical action. At the time of this report, KOT, made up of mostly young people particularly 'Gen-Z', had successfully orchestrated widespread protests against an unpopular Finance Bill 2024, leading to substantial concessions from, and ultimately complete withdrawal of the Bill[30], by the government led by William Ruto. The Bill, among others, sought to grant the Kenya Revenue Authority (KRA) sweeping powers to override data protection measures established in other laws and practices. It was not the first time this loose and yet effective group had achieved significant wins through online activism, mobilization, and coordination. In 2019, they successfully pressured then-President Uhuru Kenyatta to leave Twitter due to harsh criticism of his policies and practices[31]. That same year, they compelled the New York Times to relocate its Africa Bureau Chief, Kimiko de Freytas-Tamura[32], from Nairobi following outcry over the paper's use of an inappropriate photo, demanding, and receiving an apology.

Statistically, there's 110 percent[33] mobile phone subscriptions in Kenya (slightly more than half of those are smart phones), almost a half of the country's population is online[34], and almost a quarter[35] of it uses social media. In figures, there were 67 million mobile subscribers by the second quarter of the 2023/2024 financial year, with 34 million smart phones in use.[36] This underscores the widespread access to digital media platforms via mobile devices. This high number of smartphone users indicates a large and growing audience for digital content, with attendant risks and threats.

From the FGDs conducted, most participants are active online, all respondents use smart phones to access news and information, news and entertainment are the key content categories consumed on digital media (the quantitative 2024 MCK State of the Media study[37] agrees with this), most participants were aware of AI, and all participants agree that AI should be regulated.

Instructively, however, young people complain of being left out in digital governance issues. A young FGD participant from Mombasa claims they are not consulted on digital issues, including policy making. He cites the fact that police are unable to effectively deal with cybercrime as evidence that they do not have "young tech savvy officers among them". A KII from Nairobi also laments the absence of the youthful voice in Internet Governance issues.

In the cyber sphere, Kenya boasts a thriving ecosystem of blogs, social media platforms, and online news sites. With over 35,000[38] blogs and an active presence on platforms like Facebook, Twitter, Instagram, and TikTok, digital media has emerged as a powerful force in shaping public opinion and driving conversations. Notably, there's a gender skew, in favour of males, to social media use in Kenya. Of the 13.05 million

[29] Data Reportal (2024)

[30] Geopoll (2024); https://www.geopoll.com/blog/geopoll-report-youth-protests-in-kenya/

[31] Mwita (2021)

[32] Mwita (2021)

[33] CA (2024)

[34] Data Reportal (2024)

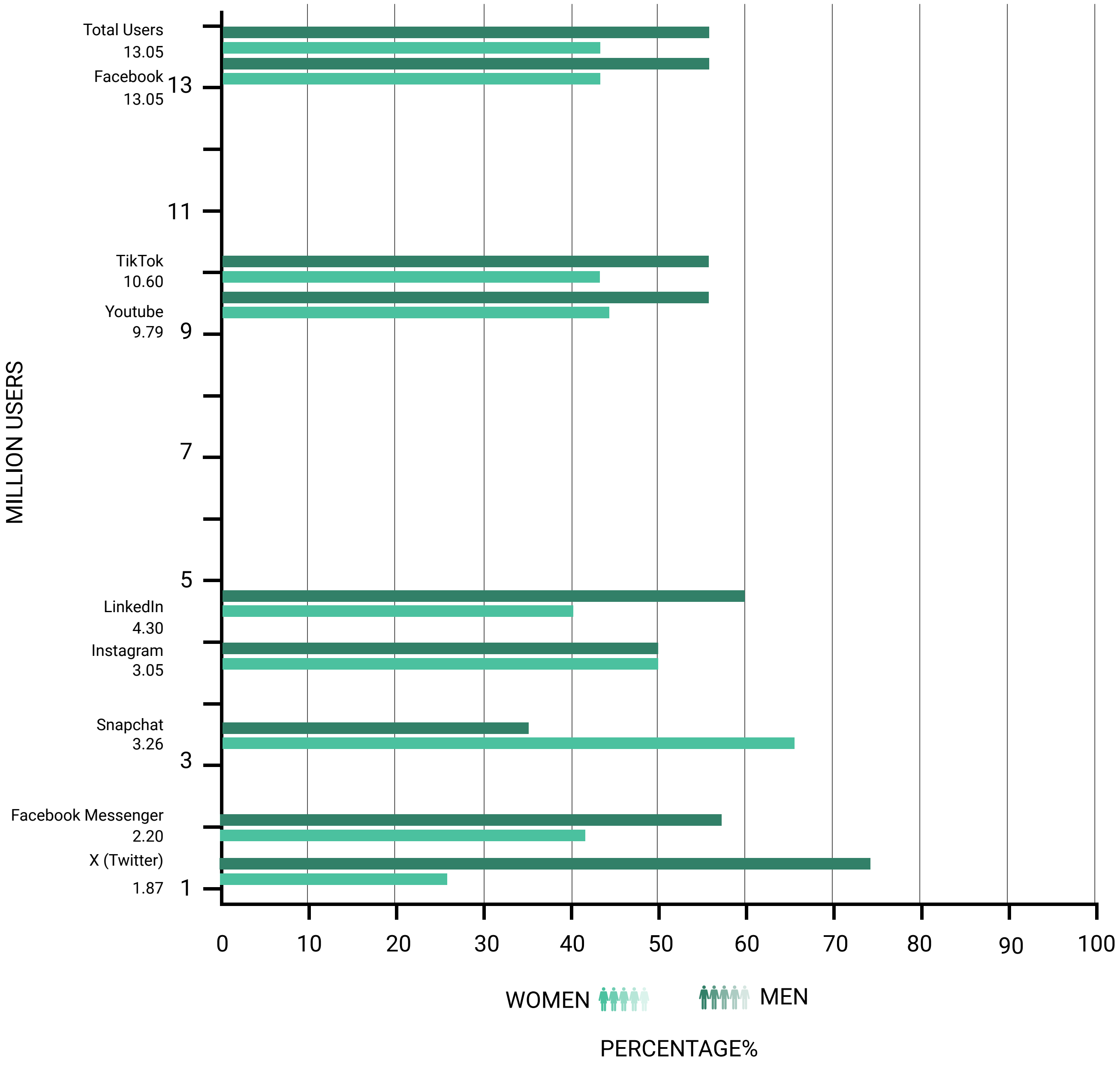
[35] Data Reportal (2024)

[36] CA (2024)

[37] MCK (2024); 'State of the Media in Kenya', Nairobi

social media users in the country as of January 2024, 56.8 percent were male while 43.2 percent were female — a sobering statistic when you consider that there are more females (50.4 percent) than males (49.6 percent) in the population of Kenya.[39] This skew is replicated on all social media platforms, except Snapchat, to varying degrees. On Snapchat, the figures are 65.9 percent female to 30.5 percent male.[40] But then Snapchat has 3.26 million users in Kenya.[41] The consolidated social media use statistics as of January 2024 are captured in the graphic below.

Graphic Generated from Data on Data Reportal 2024 Report



[38] Peter Theuri (2022), 'Bloggers thrive despite State attempts to curtail freedom', Standard, https://www.standardmedia.co.ke/nairobi/article/2001398779/bloggers-thrive-despite-state-attempts-to-curtail-freedom#:~:text=Blogs%20account%20for%20a%20majority,is%20a%20boon%20to%20bloggers., accessed June 7, 2024

[39] Data Reportal (2024)

[40] Data Reportal (2024)

[41] Data Reportal (2024)

In mapping digital sources of information, besides social media platforms, the following groups of digital sources of information came up from the FGDs:

a. Online news websites:

Online news websites, such as Citizen Digital, Nation, and Star, were said to serve as reliable sources of information for many individuals. They offer credibility, depth of coverage, and easy accessibility, allowing users to delve into various issues with comprehensive reporting. “These digital sources adhere to journalistic standards,” a participant from Kisumu said. However, the presence of paywalls, clickbait headlines, and biased reporting came up as posing challenges to users seeking unbiased and informative content. Below, is a statistical indication of how news sites perform and how news is consumed in Kenya.

Favorite news websites

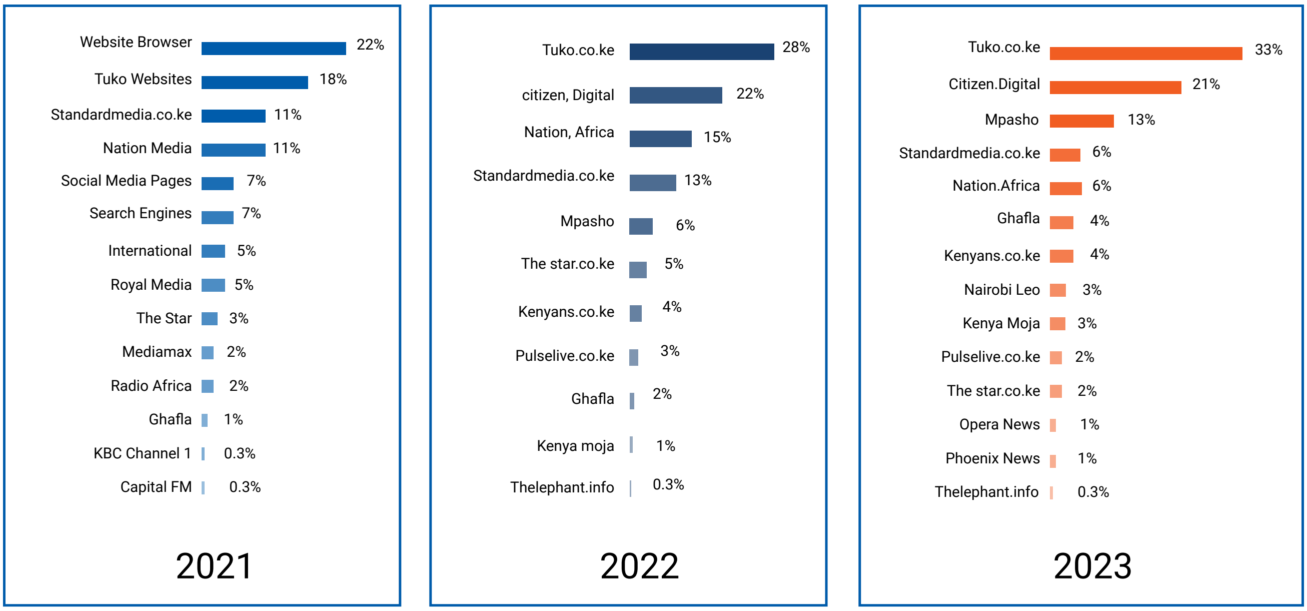


Figure 6: Performance of online news websites in Kenya. Source: MCK (2024)

b. Blogs and niche websites:

Blogs and specialised websites were said to offer niche content and foster (special interest) community engagement through interactive features like comments sections. While they provide valuable insights and a more informal tone compared to traditional news sources, concerns about credibility, limited depth, and subjective content exist. It was a significant concern that not all blogs and specialised websites adhere to journalistic standards, thus making their content shallow and deeply biased. Nonetheless, many participants found themselves drawn to them. A computer analyst from Mombasa said he uses the Gigs for Geeks to find jobs. Participants specifically mentioned bloggers Robert Alai, Cyprian Nyakundi, Silas Nyanchwani, Gabriel Oguda and Pauline Njoroge — as sources of information.

c. Email and messaging apps:

Email and messaging apps like WhatsApp and Telegram were mentioned. They facilitate direct communication, formal and informal, and fast dissemination of information. Their ability to be used for group rapid communication, information sharing, and other activities (fundraising was a major reason), render them particularly popular across the board with WhatsApp topping the list.[42] However, participants noted, they are vulnerable to spamming and the spread of misinformation, posing challenges to users seeking reliable and non-intrusive communication channels. Participants shared scam narratives of how these messaging apps were used to con or attempt to con them. In one instance there was attempted kidnapping. They also complained about receiving unsolicited or irrelevant messages, leading to information overload.

d. Artificial intelligence:

Identified by participants both as a tool as well as a source of digital information, AI was a hot topic in all the five FGDs. Participants highlighted the symbiotic relationship between humans and AI, emphasising the capacity to train AI systems to enhance productivity and creativity. ChatGPT and Grammarly were viewed as great in enhancing productivity and creativity by assisting users in writing and content generation. However, concerns about attention span decline, authenticity, and algorithmic bias raised questions about the long-term implications of AI-driven content creation. According to the FGDs, AI algorithms may perpetuate biases present in training data, leading to skewed outputs. A participant from Nakuru shared a personal experience where excessive use of AI through smartphones led to negative academic outcomes for his children — instead of focusing on classroom interactions and knowledge, they "over-relied" on Google and ChatGPT only to realise that sometimes these platforms get it wrong. He emphasised the need for curated content and parental control mechanisms to filter out harmful information, especially for young users. Instructively, participants highlighted the importance of maintaining authentic human experiences alongside AI integration to preserve human dignity.

The table below provides an overview of the digital sources of information mentioned in the FGDs, along with their respective pros and cons. Other referenced sources concur. It illustrates the diverse landscape of information consumption in Kenya's digital space and highlights the challenges and benefits associated with each source

> “ *Identified by participants both as a tool as well as a source of digital information, AI was a hot topic in all the five FGDs. Participants highlighted the symbiotic relationship between humans and AI, emphasising the capacity to train AI systems to enhance productivity and creativity.*

[42] This was not quantitatively established but every FGD participant who spoke mentioned WhatsApp.

Digital Sources of Information

PROS

CONS

Social Media Platforms
(those specifically mentioned in the FGDs are: Facebook, Twitter, Instagram, LinkedIn, Tiktok, Snapchat, Pinterest, YouTube, WhatsApp, Telegram, and Tumblr)

PROS:

- Accessibility
- Real-time updates
- Diverse perspectives
- Networking (including professional networking opportunities).

CONS:

- Misinformation
- Privacy concerns
- Biased/sensational content
- Attention span decline
- Addiction
- Vulnerability to security breaches e.g. hacking
- Expensive (cost of data bundles for connectivity)

Online News Websites
(those specifically mentioned are Nation, Citizen Digital, Radio Citizen, Standard, KTN, and Star)

PROS:

- Credibility
- Depth of coverage
- Accessibility

CONS:

- Paywalls limit free access.
- Clickbait headlines (sensationalisation)
- Biased reporting.

Blogs and Specialised Websites
(bloggers specifically mentioned were Robert Alai, Cyprian Nyakundi, Silas Nyanchwani, Gabriel Oguda and Pauline Njoroge)

PROS:

- Niche content
- Community engagement
- Informal/conversational tone.

CONS:

- Lack of credibility (lack journalistic standards).
- Limited depth
- Subjectivity.

Email and Messaging Apps
(including WhatsApp, Telegram, and Messenger)

PROS:

- Direct communication
- Fast dissemination
- Group communication and activities.

CONS:

- Security risks
- Spam
- Misinformation
- Scams and attempted scams
- Potential for information overload.

Artificial Intelligence
(specifically mentioned were ChatGPT and Grammarly)

PROS:

- Productivity enhancement
- Creativity augmentation.

CONS:

- Attention span decline
- Lack of authenticity
- Algorithmic bias
- Negative academic outcomes
- Interferes with authentic human experiences.

3. Majority of Kenyans are overwhelmed by digital onslaughts

During the FGDs, there were many narratives from participants around a 'digital onslaught'. There was a sense of helplessness and defencelessness against this onslaught. A university professor narrated how in his own house, he and his wife have put measures in place to protect their children against potential gadget misuse and online abuse and exploitation. But when their kids visit their grandmother upcountry, which is "often", the grandmother gives them her smart phone to keep them occupied and entertained. At some point he discovered that they misuse that phone by visiting inappropriate sites putting themselves at risk of online exploitation amongst other dangers. He says, there's "nothing [he] can do about it." Another participant supports by saying she once put a filter on her mother's phone to protect her children and the mother complained that she could no longer access some of the entertainment content she used to enjoy before the filter, forcing the daughter to remove the filter. She asks: "What else can I do?". A young participant from Eldoret spoke passionately about the helplessness of the information onslaught he is under. "Besides turning off my phone, there's nothing else I can do", he says. This is replicated across all FGDs held. There is a pulpable sense of resignation to these realities. One participant from Mombasa bluntly said: "AI is a reality. We just must live with it. There's no going around it."

KIIs echo this sentiment but, due to their high levels of expertise and experience, they tend to emphasise mitigation action to empower individuals and communities to safely and productively navigate through this space. "It is possible not to be overwhelmed by it all", says a KII from Nairobi. A parent speaks of limiting screen time for her children – the idea being that less screen time reduces the likelihood of a child "going down a rabbit hole". Another one speaks of only supervised access but recognises that he is powerless when not in the company of his children, "which is why educating them on safe online behaviour is important. But," he poses, "how many times do our children disobey us?" All this correspond with a huge body of literature that speaks to, for instance, an information overload and the helplessness of people in dealing with it, especially with respect to separating the truth from misinformation.

To be sure, participants and KIIs recognise the positive sides of these digital realities – ease of access to information; empowerment of marginalised communities (like the indigenous tribesman who uses social media platforms to mobilise his people, raise awareness about human rights issues, and hold authorities accountable); strengthening human rights advocacy; enhancing accountability and transparency ("With smart phones, everyone is a journalist and a watchdog against human rights abuses," a discussant from Eldoret said); innovation in education and journalism; fundraising and community patrolling (WhatsApp); and economic empowerment – but they wish they had more power to manage and make sense of it all.

4. Vague and overly broad regulations limiting digital safety and rights

Besides the National ICT policy, regulation stands as a defining feature of Kenya's media and digital landscape, shaping the operational aspects of the terrain significantly. Encompassing over 20 laws[43], these regulations exert a profound influence on various aspects of digital operations, ranging from content creation and dissemination to cybersecurity and data protection. However, the efficacy of these regulations often hinges not on their mere existence but rather on the impartial and faithful implementation thereof.

From the FGDs, and especially KIIs, Kenya faces significant policy and regulatory challenges in addressing digital threats effectively. A key area of concern lies in the cybersecurity framework, where existing policies, though established, often lack the necessary specificity and enforcement mechanisms needed to combat evolving digital threats comprehensively. This gap not only affects the implementation of cybersecurity strategies but also undermines efforts to protect against emerging risks such as phishing and ransomware attacks. Specific examples of this exists in the lack of action against repeated hacking of government digital platforms. In addition, the existing cybersecurity policies in Kenya, such as the Kenya Information and Communications Act and the National Cybersecurity Strategy, provide broad guidelines but lack detailed procedures for addressing specific threats like ransomware. These policies may outline general goals and responsibilities but fail to offer clear, actionable steps for organisations — including government — to follow when faced with such attacks. Enforcement of cybersecurity measures is also a significant challenge. For instance, while the government has established the National Computer and Cybercrime Coordination Committee (NC4), the committee lacks the resources or authority to enforce compliance effectively across all sectors. Without strong enforcement mechanisms, organisations — again, including government — may not adhere to best practices or implement necessary security measures, leaving them vulnerable to ransomware and other digital threats.

Moreover, while laws exist to address cybercrime, they may not be sufficiently robust or up to date to effectively prosecute modern forms of digital misconduct. This deficiency in legislative agility leaves gaps in legal recourse for victims and hampers the deterrence of cybercriminal activities. A specific example is the recent rise in Sim Swap Fraud, where cybercriminals manipulate mobile network systems to gain control over victims' phone numbers as was raised in the Nakuru FGD on the 'Confirm'[44] cybercriminal phenomena. The fact of the existence of another similar gang in Bomet is well-reported in the press and, importantly, formed an interesting part of FGD conversations. Sim Swap Fraud allows them to access sensitive information, such as bank account details and personal identification numbers, leading to unauthorised transactions and financial losses. "No successful prosecutions have been held on these yet due to deficiencies in legislative agility," says a KII from Mombasa.

On this, the primary legislation addressing cybercrime in Kenya is the Computer Misuse and Cybercrimes Act, 2018. While this Act covers various forms of cybercrime, its provisions do not fully encompass the sophisticated methods used in Sim Swap Fraud. For example, the Act does not explicitly address the technicalities of mobile network manipulation or the specific nature of Sim Swap scams, leading to challenges in prosecuting such cases effectively. The Act provides a framework for dealing with general cybercrime but lacks detailed guidelines for prosecuting emerging fraud schemes like Sim Swap Fraud. Prosecutors and law enforcement may find it difficult to apply the existing legal provisions to the nuanced techniques employed by fraudsters in these cases, a KII from Mombasa emphasised. This can result in delays in justice or difficulties in securing convictions. Due to these legislative gaps, victims of Sim Swap Fraud may face difficulties in seeking legal recourse. The current laws may not provide adequate remedies for victims, such as compensation for financial losses or support for recovering stolen assets. This deficiency can undermine the effectiveness of the legal system in addressing and deterring cybercriminal activities. An FGD participant in Kisumu who was a victim of this confirmed as much.

Lastly, while Kenya has enacted the Data Protection Act, gaps in its implementation and enforcement persist. Given the increasing prevalence of digital transactions and data breaches and attempts thereof[45] , reinforcing regulations around data protection and privacy is imperative to safeguarding personal information and maintaining trust in digital platforms, "something that is currently missing" as noted by a KII from Nairobi.

[43] MCK (2020); The Media Sector Legislations Review 2020; and Mwita (2021).

[44] 'Confirm' was an online criminal gang of hackers for financial fraud based in Nakuru.

[45] CA (2024)

5. An unaccountable telco and private sector

"I lost a lot of money. I kept losing more for some time even after registering the fact of having lost control of my phone line. [The bank] came for me saying I owed them money; it is money I didn't borrow but rather cybercriminals did after hijacking my line. The telecommunication provider did not refund the money I had lost through the line to fraudsters. I reported to the police but did not get any help," these are the words of a participant in the Kisumu FGD. They clearly capture the disappointment a significant portion of FGD participants had against telecommunication companies.

Participants decried lack of enforceable refund policies for telecommunication companies when it is established that customers have lost money or valuable information to cybercriminals through no direct fault of the customers. "If you lose your money in a bank and it is established that you had nothing to do with the loss, you will be refunded your money. How come telecommunication companies do not have the same rules as those of banks and yet engage in banking activities? When I lost money to a wrong number, [the telecommunication provider] said the number the money had gone to had a Fuliza loan[46] and, therefore, a refund was impossible. In short, they were forcing me to pay a loan that a cybercriminal had taken rather than absorb the loss themselves!" another participant from Mombasa said adding, "It is as if [telecommunication companies] facilitate fraud." A lawyer in the Nakuru FGD termed this as "vicarious responsibility"; one that telecommunication companies should carry.

Additionally, results from FGDs reveal a particularly vociferous dissatisfaction among PWDs towards telecommunication companies. These individuals feel neglected by service providers, as there are no provisions

[46] Unsecured loans telecommunication companies give and recover as soon as the number used to borrow the money receives any cash inflow until the loan is fully cleared.

in place to accommodate the Deaf, Dumb, or Blind. It's as if these customers are invisible to telecommunications companies.

Other service level concerns include poor connectivity (a member of an indigenous community said most of his people have no signal although they have phones — "they have to search for a signal, including climbing trees"), pricing ("my airtime and data bundles run out mysteriously" and "why should my airtime expire at all?"), poor cross network connectivity ("sometimes I am unable to call from one providers' number; it's as if one service provider filters out calls from competitors' networks" raising the possibility of anti-competition practices by the dominant provider(s)).

6. Low media and digital literacy and critical thinking skills

Media literacy being an ability to understand media messaging to make informed decisions, is low in Kenya which is why people are so vulnerable to cybercriminals, conspiracy theorists, and misinformation and disinformation purveyors, amongst others. This is compounded by low digital literacy — the skills and knowledge required to effectively use digital technologies and platforms — as exemplified by the sheer number of scamming narratives the FGDs yielded (there was at least one per participant, and there were 71 participants from across the country). Both low media and digital literacy levels speak to lack of critical thinking skills in the digital space. Critical thinking necessarily involves questioning and confirming before acting. Falling easily to fraud artists, amongst other narratives adduced, is evidence of lack of critical thinking abilities. Every participant wondered why each victim was so blind to the fact that they were being defrauded. Individuals with low media literacy skills and limited digital critical thinking abilities are likely to fall prey to all forms of online deception, as they may not adequately assess the legitimacy of messages or requests for personal information.

7. Education and journalism are the battlegrounds where the war against digital insecurity will be won or lost.

Education and journalism emerged as pivotal battlegrounds in the fight against digital threats affecting freedom of expression and personal agency rights. Concerns arose regarding AI's potential to stifle critical thinking and creativity, endangering the essence of intellectual inquiry, which some FGD participants view as a human obligation. Similarly, AI's infiltration into journalistic practices threatens to commodify truth, undermining the integrity of the Fourth Estate. The mechanisation of news reporting, driven by AI-generated content, was identified as a challenge that could undermine the authenticity and integrity of journalistic practices and adversely affect freedoms of access and expression. On the flipside, journalists in the FGDs said, in journalism, AI-powered tools streamline news production processes, automate fact-checking, and facilitate data-driven storytelling, enriching journalistic practices and promoting informed public discourse. An ordinary mother from Eldoret who spoke as a KII, leverages YouTube to enhance her children's learning. She says, not in so many words, that YouTube leverages AI algorithms to personalise learning experiences, adapt to individual learning styles, and enhance educational outcomes for her children. However, other participants expressed concerns about the overreliance on AI for academic and professional purposes, such as research and content creation. There were apprehensions that AI could lead to intellectual laziness and hinder innovation and creativity. The discussions highlighted instances where AI-generated content, including news articles and research papers, could diminish the authenticity and creativity of human-generated work. And yet, the narratives shared by participants underscored how digital technologies, particularly social media, and AI-driven analytics, have become instrumental in advancing journalism, education and human rights advocacy efforts.

Participants highlighted how digital tools facilitate information sharing, fact-checking, networking, and mobilisation, transcending geographical boundaries and empowering grassroots movements, enhancing the enjoyment of many human rights. Social media platforms were recognised as powerful tools for organising protests and campaigns (the Arab Spring was cited), thereby feeding journalism endeavours, while AI-driven analytics were seen as enabling organisations to identify patterns of human rights violations and advocate for systemic change effectively. In all this, they unanimously emphasised the place of education and journalism in educating the citizenry towards a safer and positively productive digital environment for all. "If we have to win, we must win in education and journalism first!" said a participant from Nakuru.

8. There are real life consequences for illegal or irresponsible online activity

One of the areas in which FGD participants expressed real surprise was how "innocent" online activity had devastating real-life offline consequences for people. A defrauded lady in the Kisumu FGD was stunned that some "innocent" conversation with her assumed bank could put her in such deep debt. A mother from Eldoret was on the verge of tears as she narrated how young people, "especially boys", are "innocently" led to do simple things such as share nude photos of themselves and then those are later used to blackmail them in sextortion rings. "And this has lifelong mental health consequences for the victims!" she said, wondering: "How can such a simple action lead to such consequences?” Others expressed surprise at how clicking a link “innocently” could have led to their Facebook accounts being taken over. In the Nakuru FGD, participants spoke with perplexity about the ‘Confirm’ criminal challenge. The ‘Confirm Criminal Gang’, started off as ring of hackers and online con artists in Nakuru. It was highly successful. But then, as cybersecurity efforts closed on them, they disappeared and went offline. Soon after, they emerged now as an offline gang, robbing people in their homes, in public transport vehicles, and by waylaying and robbing people on their way about ordinary life. Online, ‘Confirm’ were only hackers, physically hurting no one. Offline, they were a vicious criminal gang hurting, even, killing real people. Therefore, many digital behaviours and trends are influenced by offline factors such as socioeconomic status, education level, and cultural norms — and vice versa. These interactions and interdependencies between online and offline environments are truly intriguing.

> “ *There were apprehensions that AI could lead to intellectual laziness and hinder innovation and creativity. The discussions highlighted instances where AI-generated content, including news articles and research papers, could diminish the authenticity and creativity of human-generated work.*

Recommendations

From the analysis above, several recommendations can be put forth to enhance digital safety in Kenya. These recommendations are tailored for various stakeholders involved. For individuals, fostering digital literacy and awareness is paramount, equipping them with the knowledge to navigate online risks effectively. Organisations should prioritise robust cybersecurity measures and provide ongoing training to their staff. Policymakers are urged to enact comprehensive legislation that safeguards user privacy and holds platforms accountable for data protection. Furthermore, collaboration between stakeholders — including technology companies, international collaborators, educators, and civil society — is crucial to collectively address emerging threats and promote responsible digital citizenship. While this list is not exhaustive, these measures represent proactive steps towards creating a safer and more secure digital environment for all.

For KenSafeSpace

The KenSafeSpace project commissioned this report to serve as a foundational study, guiding strategic decisions and operational actions. Positioned uniquely, the project can directly use these findings to enhance programme impact and facilitate future scalability, ensuring effective tailoring to address identified needs and achieve sustainable outcomes:

1. Train journalists and content creators:

This is perhaps the most important thing KenSafeSpace could do as it addresses the problem on the supply side. Upholding ethical standards in content creation and journalism is essential for preserving authenticity and emotional depth amidst AI-driven automation; it can also enhance online safety by reducing misinformation and heightening professionalism and the application of ethical considerations in content creation and dissemination. This can be achieved in part through training. Content creators should adhere to principles of accuracy, transparency, and respect for users' rights and privacy. By promoting ethical content creation and dissemination practices, KenSafeSpace can help maintain trust and integrity in digital media in Kenya and mitigate the spread of harmful or misleading information.

In doing this, KenSafeSpace should not forget the place of legacy media to reach the unreached — in part as an attempt at inclusion, but also as advance preparation for their joining the digital revolution. In this, utilisation of vernacular language community radio stations with education programming on the ever-changing digital technology might help. A lot of community radio stations broadcast in vernacular languages.

2. Conduct digital media literacy and critical thinking training:

On the demand side, KenSafeSpace could target consumers for empowerment. Prioritising the development of digital media literacy and critical thinking skills is crucial for helping individuals discern between authentic, misleading, and AI-generated content for effective decision making. Educational initiatives should focus on teaching users how to evaluate sources, detect misinformation, and critically analyse digital content and players. Additionally, safety measures online such as not clicking on suspicious links should be part of such media literacy training.[47] By promoting digital media literacy, KenSafeSpace can empower many Kenyans to make informed decisions for online safety and mitigate the spread of false information online.

3. Work with policy research and engagement organisations to influence policy in the digital environment:

KenSafeSpace is in a unique position to engage stakeholders at policy level on digital safety using this research to formulate guiding topics and areas of focus. This would require partnerships with organisations whose focus of work is policy engagement such as the Kenya Institute for Public Policy Research and Analysis (KIPPRA) and KICTANet. Such engagement would entail in-depth consideration of how key media stakeholders and actors can/should be engaged in policy-formulation. The findings of this research would form the basis of such engagement resulting in memoranda, policy reviews, and policy recommendations. Comprehensive policy engagement would include actions aimed at strengthening the capacity of parliamentary caucuses and committees to engage with

[47] Please see others discussed under Recommendations for Civil Society, point number 1.

emerging digital issues and technologies including AI, to fashion appropriate changes in the legal and regulatory frameworks. This would result in policy reviews and recommendations based on, amongst others, the gaps identified under finding number 4 above (Vague and overly broad regulations limiting digital safety and rights). Of particular importance are threats facing vulnerable groups such as children, the elderly, PWDs, the youth, and women.

4. Collaborate with Government and civil society organisations in public awareness campaigns about digital security and responsible online behaviour:

Government partnerships would provide authoritative support to KenSafeSpace offering broad reach, ensuring that key messages about digital threats and safe practices are communicated widely and effectively. Civil society organisations would bring valuable grassroots insights and community trust for KenSafeSpace. Their deep understanding of local contexts would allow for the customisation of KenSafeSpace campaigns to address specific needs and behaviors of different demographics. CSOs excel in engaging with communities through workshops, training sessions, and interactive events, and collaborating with them would therefore foster responsible online behavior and personal accountability. Combining the authoritative influence of the government with the community-focused approach of CSOs would create a powerful synergy for KenSafeSpace to promote digital safety and foster lasting behavioral changes and a stronger culture of digital responsibility.

For KenSafeSpace, these recommendations are not exhaustive. As a matter of fact, each recommendation in this document is relevant to KenSafeSpace and could be actualised through targeted collaborations with different relevant stakeholders including the government, civil society, private sector, academia and youth organisations.

> “ *On the demand side, KenSafeSpace could target consumers for empowerment. Prioritising the development of digital media literacy and critical thinking skills is crucial for helping individuals discern between authentic, misleading, and AI-generated content for effective decision making.*

For the Government

Governments wield substantial influence over online behaviour and digital security through legislation, regulatory frameworks, and enforcement mechanisms. The recommendations below could be considered by the Government of Kenya to make the digital space safer:

1. Engage youth in internet governance:

From the FGDs, it was obvious that the youth are the most engaged in the digital space. Engaging youth in internet governance is, therefore, crucial for ensuring that their perspectives and concerns are represented in policy-making processes. Through education and awareness, youth forums and platforms, tailored communication, partnerships with youth organisations, policy consultations, internships and fellowships, youth advisory groups, and other continuous engagement strategies, the government can effectively engage youth in internet governance, ensuring their active participation and contributions to shaping the future and safety of the digital world.

2. Promote digital literacy:

The Government, especially through the CA's USF, should develop initiatives to enhance digital literacy, empowering individuals on appropriate digital behaviour to discern credible information from misinformation — and save themselves from online pitfalls such as fraud. By investing in digital literacy programmes and integrating them into educational curricula, the government can equip individuals with the knowledge and skills needed to protect themselves in the digital age.

3. Reform education:

Over and above infusing digital skills-building into curricular, education reform includes a deliberate thrust to move a nation into the digital age. Advocating for and instituting educational reforms that emphasise digital literacy, critical thinking, and ethical AI usage is crucial for addressing the complexities of the digital landscape. Educational institutions should integrate practical — beyond theoretical — digital literacy into their curricula and provide training for educators on teaching these skills effectively. By spearheading and prioritising digital literacy in education, the government can prepare future generations to navigate the digital world responsibly and ethically. Reform includes providing all learners with digital gadgets for practical lessons.

4. Institute ethical AI practices:

There might be efforts to develop AI policies in Kenya[48] but there is none in place. Developing and promoting ethical guidelines for AI development and deployment is essential for prioritising human well-being and rights. These guidelines should address issues such as transparency, fairness, and accountability in AI systems. By adhering to ethical AI practices, users and stakeholders can mitigate the risks associated with AI technology and ensure that it benefits society. Provisions on regular audits and assessments to identify and mitigate AI biases, discrimination, and unintended consequences in AI systems should be part of such guidelines. By implementing guidelines that prioritise human well-being and rights, the government can mitigate the risks associated with AI technology and promote responsible innovation.

> *The Government, especially through the CA's USF, should develop initiatives to enhance digital literacy, empowering individuals on appropriate digital behaviour to discern credible information from misinformation — and save themselves from online pitfalls such as fraud.*

[48] Paradigm Initiative (2024)

5. Regulate with vision:

Developing and enforcing robust regulatory measures is essential for addressing emerging digital threats while safeguarding individuals' rights coherently and effectively. These frameworks should encompass laws and policies that govern data protection, algorithmic bias, cybersecurity, and online content moderation. Telecommunications companies should be more tightly regulated to put in place failsafe refund policies, mitigate data bundle and airtime expiration dates, include PWD and child-friendly tools in service provision, and ensure universal reach. CA should be legally held responsible for lack of internet services in certain areas, for what is the multibillion-shilling USF[49] for? Regulation would include prioritisation of user privacy by adopting privacy-enhancing laws, technologies, and practices. Developing transparent privacy policies such as obtaining user consent for data collection and processing and minimising the collection of personally identifiable information would be crucial. Emphasising data anonymisation and encryption to safeguard sensitive data from unauthorised access, and enacting futuristic laws that protect human rights, considering the impact on employment, and involving stakeholder engagement cannot be gainsaid.

6. Establish an independent entity to address cybercrime:

Establishing an independent entity[50] solely dedicated to combating cybercrime offers several advantages. Firstly, such an entity would consist of experts specialised in digital forensics, cyber law, and emerging technologies, enabling a deeper understanding of complex cyber threats, and ensuring the ability to adapt to evolving tactics used by cybercriminals. Secondly, a dedicated cybercrime entity would facilitate a swift and technologically adept response to cyber incidents, reducing bureaucratic delays and preserving digital evidence effectively. This entity would serve as a central hub for coordinating efforts among various stakeholders, including law enforcement agencies, government entities, private sector organisations, and international partners. By facilitating collaboration and information sharing, the entity could identify trends, share best practices, and develop comprehensive strategies to combat cybercrime at various levels.

The establishment of a separate entity would underscore the government's stated commitment to addressing digital threats seriously, fostering public trust and confidence in cybersecurity measures. Victims of cybercrimes would feel more encouraged to report incidents, knowing that specialised professionals are available to assist them effectively. Additionally, a dedicated cybercrime entity could focus on proactive prevention strategies, such as raising awareness about cyber risks, providing cybersecurity training, conducting vulnerability assessments, and collaborating with industry partners to address systemic cybersecurity issues. By taking a proactive approach, the entity could mitigate the impact of cyber threats before they escalate into major incidents. In general, the establishment of an independent entity to combat cybercrime would lead to more effective responses to digital threats, better protection of citizens' digital rights, and increased resilience against cyber-attacks.

7. Connect the unconnected and underserved:

Bridging the digital divide, the gap between those who have access to digital technologies and those who do not, is a crucial step in addressing digital threats comprehensively. By ensuring equitable access to technology and digital literacy, the government can empower individuals and communities to navigate the digital landscape safely and responsibly. One way to address digital threats through bridging the digital divide is by providing universal access to affordable and reliable internet connectivity. This would enable underserved populations, including rural communities and low-income households, to access essential online services and information resources.

Improved access to the internet would also facilitate participation in digital literacy programmes, online education, and skill development initiatives, equipping individuals with the knowledge and tools needed to protect themselves against digital risks. The government can also invest in initiatives aimed at enhancing

[49] Sunday, F. (2024), 'CA pushes for Sh88.5b nation-wide broadband', Standard; https://www.standardmedia.co.ke/business/business/article/2001495412/ca-pushes-for-sh885b-nation-wide-broadband

[50] By entity is not meant a unit within the existing police force/criminal investigation structure, but a whole new department under a relevant the Ministry such as Interior or Communications.

digital literacy and cybersecurity awareness among vulnerable groups, such as children, the youth, the elderly, and PWDs if all are connected. These programmes could include workshops, training sessions, and educational campaigns designed to teach basic cybersecurity practices, critical thinking skills, and responsible online behaviour. By empowering individuals with the knowledge to recognise and respond to digital threats effectively, the government can strengthen overall cybersecurity resilience within society.

Furthermore, bridging the digital divide can facilitate greater inclusion and participation in digital economies, providing opportunities for socio-economic empowerment and reducing disparities in access to digital resources. By fostering innovation and entrepreneurship among underserved communities, the government can promote economic development and social mobility while simultaneously reducing the risk of digital exclusion and exploitation. Collaboration among government agencies, civil society organisations, private sector entities, and international partners is essential to effectively bridge the digital divide and address digital threats comprehensively. By pooling resources, expertise, and best practices, stakeholders can develop holistic strategies that prioritise digital inclusion, cybersecurity, and the protection of digital rights for all individuals and communities. As a scholar KII emphasised, through collective action and sustained investment in bridging the digital divide, governments and other stakeholders can create a more resilient and secure digital ecosystem for future generations. He also pointed out that although the government is making some effort in terms of manufacturing affordable devices, there is need to extend coverage by ensuring connectivity even in the far-flung areas without internet connectivity. He added that people also need digital skills to participate. He observed that you can have connectivity for the coverage of the affordable devices, but if people do not have digital skills to meaningfully use the services for productive reasons, then still the objective will not have been achieved.

For the Civil Society

In its broadest sense, civil society encompasses universities, media, NGOs, the clergy, and other organised groups outside of the government.[51] This vibrant segment of society wields significant influence over digital safety. The following recommendations are most suited for civil society action:

1. Conduct public awareness campaigns:

Implementing comprehensive education and awareness programmes is vital to equip individuals, families, and communities with the knowledge and skills needed to navigate the digital landscape responsibly. Launching awareness initiatives to educate individuals about digital threats, promote media literacy, and empower them to make informed decisions is critical for enhancing digital safety and security. These campaigns should use various channels, including social media, public events, and educational materials, to reach a wide audience. By raising awareness about digital risks and best practices for protection, civil society can empower citizens to safeguard their online experiences effectively. These programmes should cover topics such as online safety, privacy protection, and critical evaluation of digital content. Also included here would be enhanced training for law enforcement and judiciary officials equipping them with skills to investigate, prosecute and act on digital crime; public sensitisation; and engagement with tech companies. By raising awareness and promoting responsible digital citizenship, civil society stakeholders can empower users to recognise and mitigate digital risks effectively.

Awareness can be very empowering. Implementing targeted awareness campaigns to educate communities about digital threats and best practices for protection would go a long way in creating a safe digital space. Fostering collaboration between media organisations, other stakeholders, and communities to amplify awareness efforts would be useful. By raising awareness about digital risks and best practices for protection, stakeholders, especially civil society, can empower users to safeguard their online experiences effectively. Public awareness and education about cybersecurity risks and best practices also require attention. As seen, there is a notable gap in understanding among the general populace regarding the significance of protecting digital assets and recognising potential threats like phishing scams. Awareness should include exposing individuals to such safety measures as use of two-factor authentication (2FA), strong passwords, a different password for each social media account, setting up security answers, not storing passwords in insecure locations, being selective with friend requests, not following or contacting violating accounts and users, clicking links with caution, being careful about own social media

[51] Matthews, D. (1998), Politics for People: Finding A Responsible Public Voice, University of Illinois Press

postings, and becoming familiar with social media channels' privacy policies[52]. Strengthening public outreach and educational initiatives can empower individuals and organisations to adopt safer digital practices.

2. Conduct community engagement and support:

Engaging community-based initiatives, especially where community cohesion is tight, can foster digital resilience and provide support, especially for children and vulnerable populations. These initiatives may include community workshops, support groups, and online forums where users can share experiences and learn from one another. By building supportive communities and providing resources for digital literacy and safety, stakeholders can help individuals navigate digital risks more effectively.

3. Lobby for progressive digital safety laws and their implementation:

From so much of what this report says, it follows naturally, that advocating for regulatory measures to ensure cybersecurity and safeguard rights should be a key part of civil society work. Lobby for robust regulatory frameworks to address cybersecurity concerns and protect individuals' rights in the digital domain. Lobby for improved service levels of telecommunications companies and better government oversight of them. Addressing these concerns requires a concerted effort toward corporate responsibility. This entails implementing robust consumer protection measures, ensuring stringent privacy safeguards, fostering transparency in operations, and launching educational initiatives. A scholar KII underscores the pivotal role of these strategies in enhancing service levels and fostering trust between telecommunication companies and their clientele. And a civil society KII highlights the lack of proactive measures by service providers and advocates for continuous advocacy to remind them of their responsibilities. Lobby for enhanced enforcement mechanisms to hold perpetrators of cybercrime accountable. By advocating for comprehensive regulatory measures, civil society can create a more secure and transparent digital environment that upholds fundamental rights and freedoms.

For Telecommunication companies and Private Sector

The private sector applies resources with a profit motive, but alongside financial success comes a responsibility to mitigate digital threats and enhance digital safety. As custodians of vast amounts of personal and corporate data, businesses have a duty to protect sensitive information from cyber threats such as data breaches and ransomware attacks. The following recommendations are best suited for private sector action:

1. Provide empowerment and security tools to vulnerable groups:

Providing users, especially vulnerable groups such as children and PWDs, with tools and resources to control their online experiences and protect their digital rights would be a good start for telecommunication and content companies. Enabling users to report suspicious activities, abusive content, and privacy violations to relevant authorities and platforms for swift action would enhance digital safety, and the private sector can do a lot in regard.

2. Take responsibility of providing safe services:

As noted, both FGD participants and KII observed that telecommunication and social media companies have a limited role or interest in addressing cyberthreats and feel these companies could do more. Telecommunication and social media companies should increase their responsibility in enhancing online safety for their users, not just for themselves as business entities. They should embrace innovative and localized human-cantered approaches to protect digital rights to significantly enhance online safety. By investing in advanced cybersecurity infrastructure and collaborating with tech experts to develop robust safety protocols, these companies can better protect users from online threats. Specifically, telecommunication firms could spearhead initiatives that promote digital literacy and responsible online behaviour among their customers, including educational campaigns and tools for safer internet use. Partnering with regulatory bodies and non-profit organisations to support policies that address cyberbullying, data privacy, and misinformation can further bolster online safety. These actions not only demonstrate a commitment to societal well-being but also position telecommunication companies as leaders in fostering a secure and informed digital environment. Some of this is already happening but more could be done.

[52] Galal, A. (Undated)

Others

In addition, there are actions citizens — people and corporates[53] — can take individually to improve digital security. Being safe online is first and foremost, and ultimately, a personal responsibility because each individual entity is accountable for their actions and well-being anywhere. The digital space is no different. It involves understanding the risks associated with online activities, protecting personal and corporate information from misuse, and considering the broader impact of an entity's behaviour on others. Adhering to legal and ethical guidelines, staying informed about cybersecurity threats, and actively managing one's digital presence are essential for creating a safer online environment for everyone. Individuals — people and corporate — should invest in robust cybersecurity measures. These include firewalls, antivirus software, encryption, and multi-factor authentication.

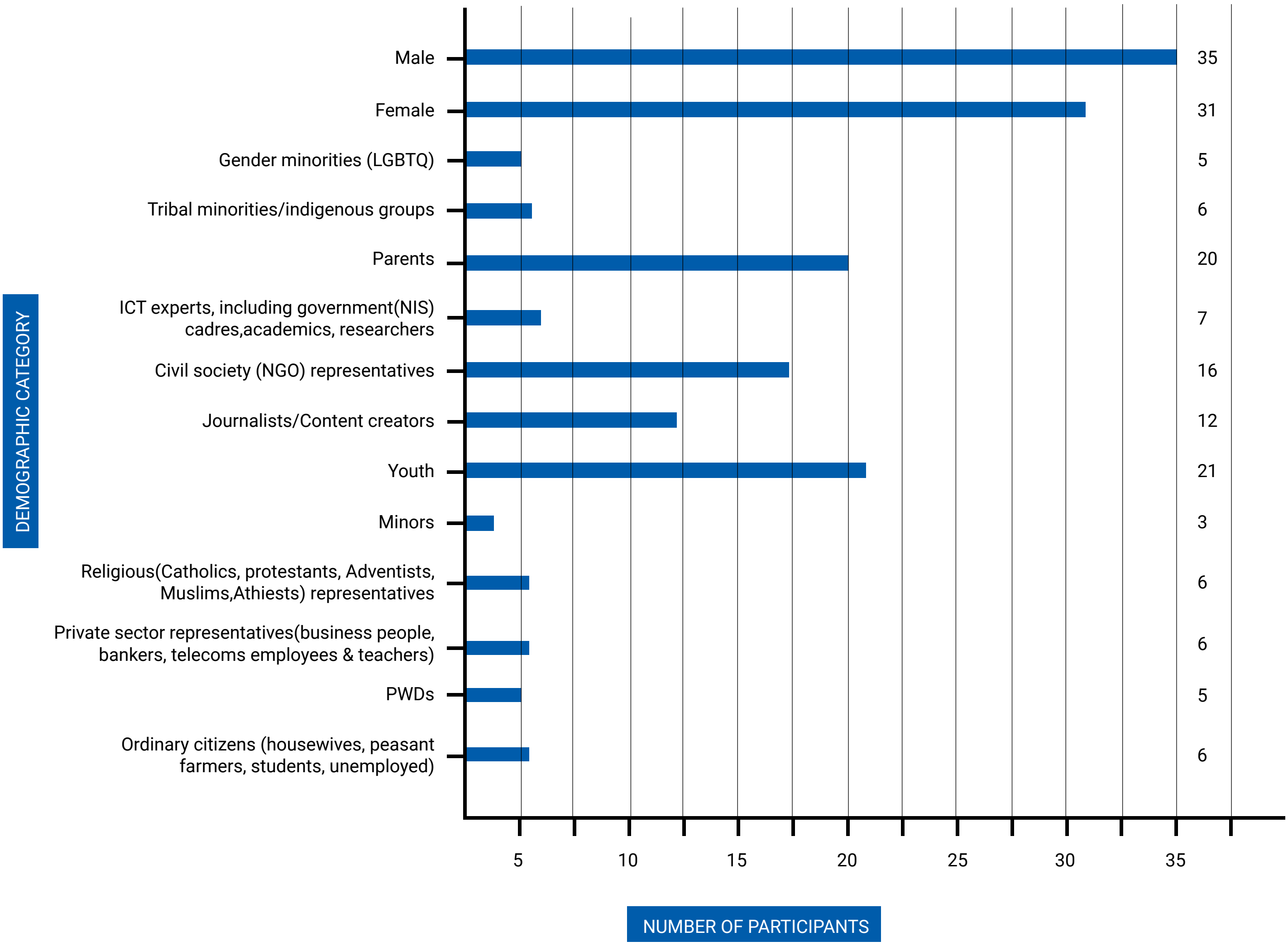
The insights and recommendations presented here underscore the complexity of digital risks and threats and the necessity for a concerted approach to address them effectively. The diverse stakeholder perspectives highlighted the importance of inclusivity in developing strategies and solutions that cater to the varied needs and interests of different stakeholders. By adopting these recommendations and fostering a collaborative, multi-stakeholder approach, we can mitigate digital risks and threats, uphold online safety, and protect human rights in the digital age.

> “ *Being safe online is first and foremost, and ultimately, a personal responsibility because each individual entity is accountable for their actions and well-being anywhere.*

[53] Corporate' in the sense of unified entities such as governments, businesses, associations etc.

Methodology

This research employed qualitative methods including literature review, key informant interviews, and focus group discussions. It applied Internews' information ecosystem assessment methodology, supplemented by CDAC Network tools for a comprehensive view. Eleven KIIs engaged stakeholders including parents, teachers, researchers, and activists. Five FGDs, spanning diverse demographics and locations (Mombasa, Nairobi, Nakuru, Kisumu, and Eldoret), provided insights into societal digital information behaviours. To ensure confidentiality and anonymity in reporting, informed consent was obtained from all the 71 participants from many different demographic categories (see table below). The research spanned five weeks, involving planning, questionnaire design, literature review, interviews, and peer-reviewed report drafting under Internews' KenSafeSpace Project Director's guidance. Below is a table representing the demographics[54] of the FGD participants and KIIs.



[54] 54. Please note: Except for gender, some participants fall under more than one category.

References

AU (2024), The Continental AI Strategy for Africa, Addis

CA (2023); https://www.ca.go.ke/universal-access-overview

CA (2024), 'Second Quarter Sector Statistics Report Financial Year 2023/2024'; https://repository.ca.go.ke/bitstream/handle/123456789/1369/Sector%20Statistics%20Report%20Q2%202023-2024.pdf?sequence=1&isAllowed=y — accessed on Monday June 24, 2024 at 10:15am

Capmad (undated), Financial Inclusion in Kenya: The M-pesa Success Story – https://www.capmad.com/technology-en/financial-inclusion-in-kenya-the-m-pesa-success-story/#:~:text=The%20company%20plays%20a%20critical,2%20%25%2C%20or%20250%2C000%20people — accessed on Monday June 24, 2024 at 11:10 am.

CDAC (2014), https://www.cdacnetwork.org/resources/communication-needs-assessments

Data Reportal (2024), 'The State of Digital in Kenya'; https://datareportal.com/reports/digital-2024-kenya

Galal, A. (Undated); Harmful Speech Watch: A Social Media Monitoring Methodology, Internews

Geopoll (2024); https://www.geopoll.com/blog/geopoll-report-youth-protests-in-kenya/

https://farmerlifeline.co.ke

https://ihub.co.ke

https://www.kictanet.or.ke

ICTA (2022), Kenya National Digital Masterplan 2022: https://cms.icta.go.ke/sites/default/files/2022-04/Kenya%20Digital%20Masterplan%202022-2032%20Online%20Version.pdf

Internews (2021), 'Internews Information Ecosystem Analysis', https://internews.org/wp-content/uploads/2021/05/Internews_Information_Ecosystem_Assessments.pdf

KICTANet (2022); Women and Data: Keeping Safe Online; https://www.kictanet.or.ke/comic-on-women-data-keeping-safe-online/

Matthews, D. (1998), Politics for People: Finding A Responsible Public Voice, University of Illinois Press

MCK (2020); The Media Sector Legislations Review 2020; and Mwita (2021).

MCK (2024); 'State of the Media in Kenya', Nairobi

Ministry of Information, Communications and Technology, Kenya (2019), National Information, Communications and Technology (ICT) Policy; https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf - accessed on Monday June 24, 2024 at 10:51 am.

Mwita, C (2021), The Kenya Media Assessment 2021, Internews, Nairobi; https://internews.org/wp-content/uploads/legacy/2021-03/KMAReport_Final_20210325.pdf - accessed on Monday June 24, 2024 at 10:25 am.

Paradigm Initiative (2024), Londa: A Digital Rights and Inclusion in Africa Report 2023, Lagos, Nigeria: https://paradigmhq.org/londa-23/

Peter Theuri (2022), 'Bloggers thrive despite State attempts to curtail freedom', Standard, https://www.standardmedia.co.ke/nairobi/article/2001398779/bloggers-thrive-despite-state-attempts-to-curtail-freedom#:~:text=Blogs%20account%20for%20a%20majority,is%20a%20boon%20to%20bloggers., accessed June 7, 2024

Sunday, F. (2024), 'CA pushes for Sh88.5b nation-wide broadband', Standard; https://www.standardmedia.co.ke/business/business/article/2001495412/ca-pushes-for-sh885b-nation-wide-broadband

Ubuntu Life (2022), Welcome to the Silicon Savannah: How Kenya is becoming the next Global Tech Hub; https://www.ubuntu.life/blogs/news/welcome-to-the-silicon-savannah-how-kenya-is-becoming-the-next-global-tech-hub - accessed on Monday June 24, 2024 at 11:05am.

Acknowledgements

We appreciate the Media Council of Kenya for their support in mobilising the participants in the FGDs in Kisumu, Mombasa, Nakuru, and Eldoret. We thank all the participants in the focus group discussions and key informant interviews for their valuable input.

KenSafeSpace

Funded by the European Union

Internews
Local voices. Global change.

KICTANet
The Power of Communities

Internet Sans Frontières

TribelessYouth

MZALENDO

Watoto Watch Network

BAKE
Bloggers Association of Kenya