Universal Periodic Review 49th Session – Kenya

Joint stakeholder report: Human rights in the digital context in Kenya

The Association for Progressive Communications (APC), a networked organisation in consultative status with ECOSOC, works to empower individuals, organisations and social movements to use information and communications technologies (ICTs) to build strategic communities to contribute to equitable human development, social justice, participatory political processes and environmental sustainability. The APC network has 73 organisational members and 41 associates active in 74 countries, including Kenya.
Contact address: PO Box 29755, Melville 2109, Johannesburg, South Africa
Website: www.apc.org
Contact person: Verónica Ferrari, Global Policy Advocacy Coordinator (veronica@apc.org)

The Kenya ICT Action Network (KICTANet) is a multistakeholder think tank for ICT policy and regulation whose guiding philosophy encourages synergies for ICT policy-related activities and initiatives. The network is a catalyst for reform in the ICT sector and is guided by four pillars: policy advocacy, stakeholder engagement, capacity building and research. The network provides mechanisms and a framework for continuing cooperation and collaboration in ICT matters among industry, the technical community, academia, the media, development partners and government.
Contact address: Nine Planets, Kabarnet Garden Road, Nairobi, Kenya, P.O. Box 14866-00880, Nairobi, Kenya
Website: www.kictanet.or.ke
Contact person: Dr. Grace Githaiga, CEO (ggithaiga@kictanet.or.ke) and Cherie Oyier, Women's Digital Rights Programme Officer (coyier@kictanet.or.ke)

KICTANet
The Power of Communities

APC
ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

I. INTRODUCTION

1. This joint stakeholder report focuses on key issues relating to human rights in the digital context in Kenya, including digital connectivity and inclusion, freedom of expression online and technology-facilitated gender-based violence (TFGBV), particularly its impact on human and women's rights defenders. The report draws on extensive and ongoing monitoring of the situation of human rights online in Kenya by a number of civil society organisations, particularly the Kenya ICT Action Network (KICTANet), and a desk review.
2. This review marks the fourth cycle for Kenya in the Universal Periodic Review (UPR) mechanism. During the third cycle, the importance of issues relating to freedom of expression, access to information, data privacy and freedom of the press was demonstrated by Kenya receiving 13 recommendations related to these issues, including two relating to data protection and the right to privacy, two on hate speech, nine relating to freedom of expression and protection of journalists and human rights defenders from attacks and intimidation, and two recommendations on access to information.[1] Commendably, the government of Kenya accepted all of these recommendations.[2]

1 Human Rights Council. (2020, 20 March). Report of the Working Group on the Universal Periodic Review: Kenya, A/HRC/44/9. https://www.ohchr.org/en/hr-bodies/upr/ke-index

2 Ibid.

II. CONTEXT OF THE SITUATION OF HUMAN RIGHTS ONLINE IN KENYA

3. Human rights online in Kenya has been adversely affected in 2024 by the government's response to the recent public protests to do with #RejectFinanceBill2024. Social media played a critical role in mobilising protestors and coordinating efforts, but also in being a place for protest in its own right.[3] There was a widespread and harsh crackdown on the protests, including arrests and abduction of protestors and human rights defenders, facilitated by use of geospatial data, internet shutdowns and curtailment of press and media freedoms, as will be further detailed in subsequent sections. Some 50 protestors were reported killed and over 400 injured during the police crackdown, many as a result of police firing live ammunition on protestors.[4]
4. Similarly, hate speech and information manipulation circulating online before and after the August 2022 general elections contributed to Freedom House lowering Kenya's Freedom on the Net rating in 2023, rating it as "Partly Free" with a score of 66/100.[5] Since its UPR review during the third cycle, Kenya has made progress towards implementing some of the recommendations received. The Kenya Data Protection Act 2019 came into effect in November 2019, with progress towards implementation beginning in 2020.[6]

3 APCNews. (2024, 19 July). Digital protests, access and freedoms in Kenya. *Association for Progressive Communications*. https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya

4 Mute, D. (2024, 16 July). Statement on Mukuru Murders and Updates on the Anti-Finance Bill Protests. *Kenya National Human Rights Commission*. https://www.knchr.org/Articles/ArtMID/2432/ArticleID/1201/Statement-on-Mukuru-Murders-and-Updates-on-the-Anti-Finance-Bill-Protests

5 Freedom House. (2023). *Freedom on the Net 2023: Kenya*. https://freedomhouse.org/country/kenya/freedom-net/2023

6 https://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN264_2021.pdf

III. DIGITAL ACCESS AND INCLUSION

5. Kenya's connectivity landscape has significantly evolved over the past decade, marked by the establishment of six submarine fibre cables that link the country to global networks. These cables – SEACOM, TEAMS, EASSy, LION2, DARE1 and PEACE – have enhanced international bandwidth and facilitated the growth of internet services across the nation. However, despite these advancements, a pronounced digital divide persists, particularly at the last mile, where access remains limited for many rural and underserved communities.[7]
6. Kenya's internet penetration is currently estimated to be 56.03%. Many Kenyan websites fall short in terms of accessibility. According to the Mobile Gender Gap Report 2023, only 39% of Kenyan women and 59% of men have access to the internet.[8] These significant digital divides, including the under-representation of marginalised groups online, impact not only access to the internet, but also financial inclusion, access to education and the like. For instance, persons with disabilities face many barriers in accessing financial products and services, including lack of accessibility of digital channels.[9] This contributes to cybercrimes such as financial fraud against persons with disabilities who need assistance in accessing the internet. According to the KICTANet Accessibility Scorecard 2023, several critical government websites scored below average in accessibility.[10]
7. There is also a rural-urban divide in terms of available infrastructures and economic barriers to access to devices and data bundles.[11] Most internet users are concentrated in urban areas, leaving rural regions with limited access to reliable internet services. Approximately 71% of Kenyans live in rural areas, where internet access is often inadequate.[12]
8. Outages and disruptions in internet services also occasionally occur. Frequent electricity interruptions caused by ageing infrastructure and deteriorating supply lines also lead to interruptions in home internet access.[13] Under the Kenya Vision 2030 development plan, the government has prioritised the expansion of information and communication technology (ICT) capacity, including plans to expand the country's optic fibre infrastructure and internet connectivity.[14] High costs of accessing the internet also remain a major barrier to universal digital access. Access remains prohibitively expensive for much of the population, despite significant investments meant to improve rural connectivity.[15] A report by the Friedrich Naumann Foundation found that the high cost of data excludes lower-income Kenyans from benefiting from the digital economy.[16]

---

7 Internet Society. (2024, 23 July). 2024 East Africa Submarine Cable Outage Report. https://www.internetsociety.org/resources/doc/2024/2024-east-africa-submarine-cable-outage-report

8 GSMA. (2023). *The Mobile Gender Gap Report 2023*. https://www.gsma.com/r/wp-content/uploads/2023/07/The-Mobile-Gender-Gap-Report-2023.pdf

9 Angwenyi, V., et al. (2023). *Financial inclusion for persons with disabilities in Kenya: A rapid review and qualitative study.* Sightsavers. https://research.sightsavers.org/wp-content/uploads/2023/07/Sightsavers-research-centre-financial-inclusion-for-persons-with-disabilities-in-kenya-final-report-july-2023.pdf

10 Awino Ouma, F., Nyakundi, N., & Okite, J. (2023). *Accessibility of Government Websites to Persons with Disabilities: Scorecard*. KICTANet. https://www.kictanet.or.ke/?mdocs-file=48324

11 Okello, F. (2023). *Bridging Kenya's Digital Divide: Contexts, Barriers and Strategies*. CIGI Digital Policy Hub. https://www.cigionline.org/static/documents/DPH-Paper-Okello.pdf

12 Awino, F. (2023, 18 June). Digital Divides and Inclusion: How are Things? *KICTANet*. https://www.kictanet.or.ke/digital-divides-and-inclusion-how-are-things

13 Freedom House. (2023). Op. cit.

14 https://vision2030.go.ke/about-vision-2030

15 Freedom House. (2023). Op. cit.

16 Ndemo, B., & Thegeya, A. (2023). *From Mobile Money to Digital Cash: Learning from Africa's Experience with Mobile Money for the Introduction of Central Bank Digital Currencies*. Friedrich Naumann Foundation for Freedom. https://shop.freiheit.org/#!/Publikation/1418.

9. In 2023, Starlink was launched in Kenya, offering lower internet costs. However, this launch has faced opposition from rival mobile network operators (MNOs) such as Safaricom, who argue that allowing satellite service providers without physical presence in Kenya poses potential security risks. Safaricom proposed that in order to tackle these potential risks, the Communications Authority of Kenya, the telecoms regulator, mandate foreign satellite service providers to partner with local MNOs if they are to enter the market.[17] A case has since been filed in court by Kituo Cha Sheria, a local NGO, challenging Safaricom's position and arguing that cheaper internet costs impact access to essential services that enable individuals to participate in the global economy and exercise their fundamental rights and freedoms.[18]
10. The Kenyan government has made progress in digitising public services, claiming to have transitioned 5,084 government services online as of mid-2023.[19] The digitisation of government services and implementation of the digital ID regime in Kenya raises significant concerns regarding digital inclusion, particularly for marginalised populations and those in rural areas.[20] In the Huduma Card case of 2020, a three-judge bench ruled the Huduma ecosystem unconstitutional, citing its inadequacy in addressing issues of exclusion and data privacy concerns.[21] The court recommended the establishment of robust regulatory frameworks to tackle barriers such as access to identity documents, the distance to administrative offices and other related challenges. Similarly, the new Maisha Namba digital ID regime has faced criticisms over concerns around privacy and digitisation of exclusion.[22] There are questions surrounding government transparency on data protection impact assessments (DPIAs), which could indicate actions being taken to minimise privacy rights violations when implementing the Maisha Namba system. Finally, critics fear that automated decision making in the digital ID regime may further marginalise communities such as the Somali and Nubian populations, who would face additional challenges in accessing public services such as healthcare and education.[23]
11. The digitisation of public services and processes risks leaving behind communities that lack internet access, even as those with connectivity benefit from these advancements, sharpening the digital divide. It is crucial for policy makers to address these challenges by executing strong privacy protections and mitigating exclusion to cater to the diverse needs of all, particularly the most marginalised.
12. All stakeholders, especially the government, must strengthen regulatory efforts, collaborative strategies and commitment to fortify digital foundations aimed at nurturing a secure and inclusive digital environment. Expanding meaningful connectivity, especially with a focus on community-driven solutions, is key to ensuring plurality and diversity, allowing all Kenyans to equally access the internet.

---

17 Joseph, P. (2024, 28 August). Safaricom 'calls for' mandated MNO-SatCo partnerships as Starlink expands in Africa. *TelcoTitans*. https://www.telcotitans.com/vodafonewatch/safaricom-calls-for-mandated-mno-satco-partnerships-as-starlink-expands-in-africa/8413.article

18 Kiplagat, S. (2024, 6 September). Kituo takes on Safaricom over Starlink Kenya entry claims. *Business Daily*. https://www.businessdailyafrica.com/bd/corporate/companies/kituo-takes-on-safaricom-over-starlink-kenya-entry-claims-4752004

19 Kinyanjui, M. (2023, 31 July). We've Fully Digitised 5,084 Government Services – Owalo. *The Star*. https://www.the-star.co.ke/news/2023-07-31-weve-fully-digitised-5084-government-services-owalo

20 CIPIT & Amnesty International Kenya. (2023). *Digital ID in Kenya: An Advisory Policy Paper Providing a Roadmap to the Implementation of a Rights-Respecting Digital ID Regime in Kenya*. https://www.amnestykenya.org/wp-content/uploads/2024/01/Digital-ID-in-Kenya-FINAL-POLICY-PAPER_Print.pdf

21 King'ori, M. (2022, 8 February). How the Kenyan High Court (Temporarily) Struck down the National Digital ID Card: Context and Analysis. *Future of Privacy Forum*. https://fpf.org/blog/how-the-kenyan-high-court-temporarily-struck-down-the-national-digital-id-card-context-and-analysis

22 Walubengo, J. (2023, 10 November). Understanding Masha Naimba: Kenya's New Digital Identity System. *KICTANet*. https://www.kictanet.or.ke/understanding-maisha-namba-kenyas-new-digital-identity-system/

23 Waswa, V. (2024, 15 September). Maisha Namba Project: A Balancing Act between Modernization and Public Trust. *KICTANet*. https://www.kictanet.or.ke/maisha-namba-project-a-balancing-act-between-modernization-and-public-trust/

13. Regulatory frameworks in the country must allow for the diversification of the connectivity providers ecosystem and the coexistence of different economic and organisational models for internet connectivity provision, including community networks and medium and small cooperative service providers or operators. Financing mechanisms for universalisation of connectivity must be designed and implemented to benefit small and community-based actors.
14. It is commendable that community networks have been included within the country's regulatory frameworks. The country has established a Community Network Service Provider (CNSP) Licence, specifically designed for not-for-profit entities.[24] The establishment of the licence reflects a significant step towards enabling community-driven telecommunications solutions. This licensing framework was developed with technical support from civil society organisations and academia, such as APC, KICTANet and the University of Strathclyde, focusing on shared spectrum management and operational guidelines.
15. The draft Universal Service Fund (USF) Strategy 2022-2026 proposes the establishment of 100 community networks within five years, specifically targeting areas that lack sufficient connectivity, and it is looking to adopt financing mechanisms that will support community networks and other complementary connectivity providers.[25]
16. The digital gender divide is also manifested in the poor representation of women in ICT courses and digital technology jobs. In Kenya, women hold less than 30% of jobs related to digital technology. The root cause of the problem can be traced to disadvantages that girls and young women accumulate throughout their years in education, with less than 30% of ICT graduates being women.[26] The reasons for low enrolment in ICT courses include the negative impact of gendered social norms, poor advocacy of digital technology careers to girls and inadequate vocational counselling.[27]
17. Action to address this divide also requires workable strategies to ensure that girls take up more ICT classes and courses. This necessitates the revival and earnest implementation of government initiatives such as the laptops-for-schools programme, the 2016 digital literacy programme and the coding-for-schools initiative aimed at enhancing digital literacy and ICT skills, which would contribute to bridging the gender divide in the ICT workforce. More needs to be done to encourage girls to take up ICT courses, promote affirmative action strategies to hire more women in the ICT sector and implement policies that promote equal pay, fair working conditions and putting in place anti-sexual harassment measures.[28]

---

24 https://www.ca.go.ke/sites/default/files/CA/Licenses%20Templatses/Community%20Network%20and%20Service%20Provider%20Licence.pdf

25 https://www.ca.go.ke/sites/default/files/CA/Universal%20Access/Draft-USF-Strategic-Plan-2022-2026-.pdf

26 Luvanda, A. (2023). *Bridging the Gender Divide in Digital Technology Courses and Careers in Kenya*. Center for Universal Education at Brookings. https://www.brookings.edu/wp-content/uploads/2023/02/Brookings2022-KenyaFinal-WEB.pdf

27 Luvanda, A. (2022, 14 December). How more girls and young women can participate in Digital Technology Courses and Careers in Kenya. *Brookings*. https://www.brookings.edu/articles/how-more-girls-and-young-women-can-participate-in-digital-technology-courses-and-careers-in-kenya/

28 Oyier, C. (2024, 25 April). Bridging the Digital Divide: How Kenya Can Empower Girls in ICT. *KICTANet*. https://www.kictanet.or.ke/bridging-the-digital-divide-how-kenya-can-empower-girls-in-ict/

IV. FREEDOM OF EXPRESSION ONLINE

Criminalisation of online speech

18. Kenyan laws continue to contain provisions that unduly restrict free speech and expression online, those under the Computer Misuse and Cybercrimes Act, 2018 (known as the Cybercrimes Act). Though the law was designed to "outlaw the abuse of people on social media", it has been critiqued as providing a back door to government-led censorship and repression of human rights online.[29] Sections 22 and 23 of the Cybercrimes Act criminalise false publication and the false publication of information online "that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person *(sic)*," with the offender being subject to imprisonment of up to 10 years.[30] Though a number of problematic provisions of the Cybercrimes Act were challenged before the High Court, the case was eventually dismissed by the court, which upheld the constitutionality of the act.[31] An appeal against this decision to the Court of Appeal remains pending.
19. Sections 22 and 23 of the Cybercrimes Act have been used to target bloggers. In 2020, blogger Cyprian Nyakundi was arrested and charged under Section 23 for posting some information on his Twitter account. In 2021, another blogger, Edgar Obare, was arrested and charged under the same law for an exposé on his social media accounts.[32] During the COVID-19 pandemic, several bloggers and social media users were arrested under the same law, for allegedly spreading false information online, including misinformation about the pandemic.[33] On 1 October 2024, David Morara Kebaso, a political activist and government critic, was arrested and charged under Section 27 of the Cybercrimes Act for content posted on his X account.[34]
20. On 18 September 2024, the National Assembly of Kenya received a bill aiming to amend the Cybercrimes Act, including Section 27. Unfortunately, the proposal seeks to expand the scope of the offence of cyber harassment.[35]
21. Such cybercrime legislations that are characterised by broad and vague definitions, contrary to the principles of legality, necessity and proportionality, allow for arbitrary or discretionary application and result in legal uncertainty, presenting serious dangers to the exercise of fundamental rights due to their criminalising effects which, in turn, deepen inequalities.[36] Cybercrime legislation should be used solely for addressing offences that require the use of a computer system – the so-called "cyber-dependent" crimes, such as hacking, denial-of-service attacks, and ransomware.

---

29 APCNews. (2019, 16 January). Internet Shutdowns Africa: It was like being shut off from the world. *Association for Progressive Communications*. https://www.apc.org/en/news/internet-shutdowns-africa-it-being-cut-world

30 https://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

31 Bloggers Association of Kenya v. Attorney General & Others [2020] eKLR - Petition 206 of 2019. http://kenyalaw.org/caselaw/cases/view/191276

32 Kapiyo, V. (2024). *Surveillance Laws and Technologies Used in Countering Terrorism and their Potential Impact on Civic Space*. KICTANet. https://www.kictanet.or.ke/?mdocs-file=49126

33 Ibid.

34 Wycliffe, M. (2024, 1 October). Uproar as Kenyan activist in court over cyber-crime. *BBC*. https://www.bbc.com/news/articles/c1wngd0d0n2o

35 http://parliament.go.ke/sites/default/files/2024-09/THE%20COMPUTER%20MISUSE%20AND%20CYBERCRIME%20(AMENDMENT)%20BILL%2C2024.pdf

36 Derechos Digitales & Association for Progressive Communications. (2023). *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks*. https://www.apc.org/sites/default/files/gender_considerations_on_cybercrime_0.pdf

The extension of cybercrime legislation to cover "cyber-enabled" crimes (traditional offences committed using a computer) is unnecessary and risky to a number of human rights.[37] Cybercrime frameworks that consider "cyber-enabled" crimes a content-related offence, which could result in "panic, chaos, or violence", and publishing false information online with lack of precision in provisions can lead to these frameworks being often used to prosecute a broad range of online expression, censoring, and criminalising online speech and affecting human rights.[38]

22. On a positive note, Section 77 of the Penal Code, which created the offence of "subversion" and criminalised acts done or words spoken with a subversive intention, was struck down as unconstitutional by the High Court of Kenya in March 2024. The case followed the arrest of Joshua Otieno Ayika, who was charged with subversive activities for a tweet during the 2023 cost-of-living protests, predicting a governmental takeover by the army within 90 days.[39] The High Court found that Section 77 of the Penal Code was vague, overbroad and lacked clarity regarding purpose and intent, deeming it unnecessary in a democratic society.[40] Earlier, in May 2021, the High Court had also struck down Section 66 of the Penal Code, which barred the publication of false information, on similar grounds, for violating the right to freedom of expression under the Kenyan Constitution.[41] However, as highlighted above, a similar offence of publishing false information online continues to exist under the Cybercrimes Act.

Arrests and intimidation of human rights defenders and journalists

23. The recent reported cases of abduction and killing of dissenting voices and journalists are extremely concerning, such as the case of Daniel Muthiani alias Sniper, who was a political blogger known to criticise the Meru County governor and her administration until his death. Muthiani was lured from his home in December 2023 through a call allegedly setting up a meeting with the said governor, after which he was abducted and found dead with his body floating in a river.[42] This follows the death of Pakistani journalist, Arshad Sharif, in October 2022, after he was shot by a police officer in a remote area outside Nairobi.[43]

24. Arrests and abductions of journalists and human rights defenders, often facilitated by use of geospatial data, have a chilling effect on the free speech of protestors, human rights defenders and citizen activists using online platforms to exercise their rights to freedom of expression, demonstration and picketing. An escalating number of such cases have been reported in recent years, particularly related to mass protests against the government.

---

37 Ibid.

38 Hakmeh, J., & Saunders, J. (2024, 11 July). The Strategic Approach to Countering Cybercrime (SACC) Framework. *Chatham House*. https://www.chathamhouse.org/2024/07/strategic-approach-countering-cybercrime-sacc-framework/introduction

39 Kiprono, D. (2024, 29 March). Court Ruling Recognizes Freedom of Expression as an Instrumental Right. *International Commission of Jurists*. https://icj-kenya.org/news/court-ruling-recognises-freedom-of-expression-as-an-instrumental-right.

40 KICTANet. (2024, 19 March). Kenyan High Court declares s.77 of the Penal Code Unconstitutional. https://www.kictanet.or.ke/kenyan-high-court-declares-s-77-of-penal-code-unconstitutional/

41 Muthoni, K. (2021, 13 May). Telling rumours, publishing false statements is not criminal offence – Court. *The Standard*. https://www.standardmedia.co.ke/national/article/2001412719/why-you-won…

42 Wanga, S. (2024, 8 May). How Slain Meru blogger 'Sniper' was lured to his death. *The Standard*. https://www.standardmedia.co.ke/national/article/2001494743/how-slain-meru-blogger-sniper-was-lured-to-his-death

43 ARTICLE 19. (2024, 19 July). Kenya: Safeguard freedom of expression for sustainable development. https://www.article19.org/resources/kenya-safeguard-freedom-of-expression-for-sustainable-development/

25. The recent public protests in Kenya relating to the Finance Bill 2024, which was a legislation aiming to increase taxes, saw an ensuing police crackdown. Reporters faced numerous instances of physical assaults, arrest and detention. Dozens of cases of journalists attacked during the protests were documented by the International Press Institute, with the police allegedly attacking journalists with impunity under the guise of dispersing protestors.[44]
26. In April 2023, the Kenya Media Sector Working Group documented more than 20 cases of attacks against journalists, including harassment, arbitrary arrests and physical attacks, while covering mass anti-government protests that were taking place in March-April 2023. Significantly, state actors were found to be responsible for or encouraging many of these attacks.[45] Police officers were documented to have inflicted physical attacks on journalists, confiscating their valuables, and destroying their equipment and information collected by them.[46]
27. Worryingly, the Kenyan government is in fact introducing new legislation to further criminalise online speech and assembly. The Kenya Assembly and Demonstrations Bill, introduced before the National Assembly, seeks to regulate assemblies using vague grounds of "public safety" and "public order". The bill makes it a criminal offence for a person to take part in an "unlawful assembly" without clearly defining the term.[47] This provision will create a chilling effect on people's ability to engage in peaceful assemblies online, which in the past have been found to include activities such as crowdfunding, using social media for mobilisation of protests, as well as using online spaces as places of assembly to strategise on organising protests.[48] Online crowdfunding for these purposes is further threatened by the introduction of the Public Fundraising Appeals Bill, 2024 which aims to introduce permits that must be obtained before conducting public fundraising activities, among other restrictions.[49]

Shutdowns, blocking, censorship and access

28. Kenya experienced one of its first internet shutdowns in November 2023, when the government blocked Telegram for a week during national examinations. This raised fears among the public and civil society of potential internet shutdowns during the public protests against the Finance Bill 2024. Despite the Communications Authority publicly stating on 24 June 2024 that they had no intention of shutting down the internet during protests, Kenya experienced widespread internet outages the following day.[50] Though telecommunications companies sought to explain the source of disruptions as outages in undersea cables, this has been met with scepticism.[51]

---

44 International Press Institute. (2024, 27 June). Kenya: Attacks on journalists must stop. https://ipi.media/kenya-attacks-on-journalists-covering-protests-must-stop/

45 ARTICLE 19. (2024, 19 July). Op. cit.

46 Media Council of Kenya. (2023, 27 March). Mass Action that Attacks Media is Self-Defeating and Threatens Democracy. https://mediacouncil.or.ke/sites/default/files/advisory-press-releases/Press%20Statement-%20Mass%20Action%20that%20Attacks%20Media%20is%20Self%20Defeating%20and%20Threatens%20Democracy.pdf

47 http://www.parliament.go.ke/sites/default/files/2024-06/THE%20ASSEMBLY%20AND%20DEMONSTRATION%20BILL%2C2024.pdf

48 Access Now & KICTANet. (2024, 9 September). Joint Memorandum on the Assembly and Demonstrations Bill 2024. https://www.accessnow.org/wp-content/uploads/2024/09/Access-Now-and-KICTANet_-Joint-Memorandum-on-Assembly-and-Demonstrations-Bill.pdf

49 http://www.parliament.go.ke/sites/default/files/2024-08/BILL%20DIGEST%20FOR%20THE%20PUBLIC%20FUNDRAISING%20APPEALS%20BILL%202024.pdf

50 APCNews. (2024, 19 July). Op. cit.

51 Abiero, D. (2024, 9 August). Technology-Facilitated Rights and Digital Authoritarianism: Examining the Recent Internet Shutdown in Kenya. *CIPIT*. https://cipit.org/technology-facilitated-rights-and-digital-authoritarianism-examining-the-recent-internet-shutdown-in-kenya/

29. Internet shutdowns, censorship and other internet controls violate the fundamental rights of freedom of expression, access to information and picketing, which are guaranteed under Kenya's Constitution, as well as under international human rights law.[52] Internet disruptions also subvert democratic purposes by preventing people from engaging in public conversations and holding the government to account. Internet blackouts could also have disastrous economic implications, including severely disrupting Kenya's thriving e-commerce business, and rendering inaccessible mobile money services like M-pesa, and credit and debit card transactions, on which millions of Kenyans depend for daily banking transactions. Further, internet shutdowns hinder emergency services and access to vital information during crises.[53]
30. With regard to blocking, the Kenyan parliament was considering banning TikTok. This recommendation arose after the then Interior and National Administration Minister Kithure Kindiki (now deputy president) accused the platform of being used to spread propaganda, carry out fraud and distribute sexual content.[54] This recommendation has been shot down with an alternative one advocating stricter oversight by regulators such as the Communication Authority and the Office of the Data Protection Commissioner through a co-regulation model.[55]

Economic barriers to freedom of expression online

31. Amendments to the Finance Act in 2023 introduced a 15% tax on the earnings of digital creators and influencers.[56] Content creators have criticised this tax on the grounds that it curtails the right to freedom of expression due to the economic barriers it places on the freedom of expression which includes the freedom of artistic expression.
32. In a similar vein, in May 2024, the Kenya Film Classification Board (KFCB) gave a directive requiring monetised YouTube content creators to submit their videos to it for examination and classification before they are shared with the public. The KFCB argues that this is in line with the Films and Stage Plays Act, as audiovisual content uploaded to YouTube should be classified as films, which require licences from the KFCB before exhibition and distribution to the public.[57] This directive has since been challenged and the petition is still pending in court.[58] This directive would see Kenyan people being forced to pay licensing fees for videos that do not really earn them a living, thereby curtailing the right to freedom of artistic expression.

---

52 KICTANet et al. (2024, 27 June). #KeepItOn – Preserving Digital Rights and Economic Prosperity: A Call against Internet Shutdowns in Kenya during #RejecttheFinanceBill Picketing. *APC*. https://www.apc.org/en/pubs/keepiton-preserving-digital-rights-and-economic-prosperity-call-against-internet-shutdowns

53 Ibid.

54 Mihiri, D. (2024, 21 March). Kenya tells Tiktok to show it is complying with privacy laws. *Reuters*. https://www.reuters.com/technology/kenya-tells-tiktok-show-it-is-complying-with-privacy-laws-2024-03-21/

55 Mihiri, D. (2024, 25 April). Kenyan government recommends regulating, not banning, Tiktok. *Reuters*. https://www.reuters.com/world/africa/kenyan-government-recommends-regulating-not-banning-tiktok-2024-04-25/

56 DW. (2023, 27 October). Kenya: New tax frustrates digital content creators. *DW*. https://www.dw.com/en/kenya-new-tax-frustrates-digital-content-creators/a-67225726

57 Gachie, K. (2024, 24 May). Uproar as KFCB now demands Youtube Content Creators to get licences. *Citizen Digital*. https://www.citizen.digital/entertainment/uproar-as-kfcb-now-demands-youtube-content-creators-get-licences-n342758

58 Gitonga, N. (2024, 10 June). Content creators challenge KFCB licensing directive. *The Sunday Standard*. https://www.standardmedia.co.ke/nairobi/article/2001496926/content-creators-challenge-kfcb-licensing-directive

Disinformation and misinformation

33. The spread of disinformation online also has grave implications on the right to freedom of expression online. Disinformation has taken many different forms – with one of the most critical being gendered disinformation,[59] a specific type of violation of women's rights that particularly affects their freedom of expression, and the use of deepfakes to manipulate images to depict explicit sexual images or to otherwise discredit women leaders. For instance, during the 2022 general election, trolls used disinformation to target a candidate for deputy president, Martha Karua, which led to increased online abuse and harassment against her.[60]

34. The widespread use of AI-generated deepfakes on social media to spread disinformation has also been documented in various circumstances in Kenya. As noted above, it has been used to discredit political candidates, including for instance, a digital card depicting Polycarp Igathe, Nairobi's 2022 gubernatorial candidate, as uttering words with sexual undertones, which has since been denounced as a deepfake.[61] Such AI-generated content was being used to depict the #RejectFinanceBill2024 as an LGBTQIA+ agenda, with the aim of discrediting the cause.

35. Online disinformation tactics posed significant difficulties in verifying information and countering misleading claims. This was particularly the case during periods when the internet was shut down, as the ensuing information vacuum allowed disinformation to spread unchecked. Following Kenya's anti-tax protests, for example, there were alarming claims about a massacre in Githurai with reports alleging over 200 deaths – spread through videos showing gunfire and police presence, and old footage from a massacre in Ghana.[62] The claims were eventually disproved by a BBC investigation.[63]

36. Government authorities expressed concern about the use of disinformation during the #RejectFinanceBill2024 by activists, though in many cases it was used as a countermeasure for targeting, harassment, and infringement of the right to demonstrate and picket.[64] Meanwhile government agencies and mandate holders also faced backlash from the public for adoption of online disinformation tactics during the #RejectFinanceBill2024 to discredit the protesters' cause. For example, some members of parliament falsely declared that photos of the Occupy Parliament protest were digitally altered to drive the narrative of the protests, while others claimed that the protests were merely aimed at fuelling views on social media such as TikTok for content creators.[65]

---

59 Martins, P. (2024). *Placing "gender" in disinformation*. Association for Progressive Communications. https://www.apc.org/en/pubs/placing-gender-disinformation

60 Ngari, L. (2024, 25 April). How gendered disinformation on social media harms Kenyan women taking public office. *Advox Global Voices*. https://advox.globalvoices.org/2024/04/25/how-gendered-disinformation-on-social-media-harms-kenyan-women-seeking-political-office/

61 Amantika-Omondi, F. (2022). The Regulation of Deepfakes in Kenya. *Journal of Intellectual Property and Information Technology Law, 2*(1), 145-186. https://journal.strathmore.edu/index.php/jipit/article/download/208/227/612

62 Abiero D. (2024, 9 August). Op. cit.

63 Soy, A. (2024, 29 June). Was there a massacre after Kenya's anti-tax protests? *BBC*. https://www.bbc.com/news/articles/c25l14wpkryo

64 Weetracker. (2024, 5 July). AI Use Worries Kenyan Officials As Digital Tools Help Fuel Anger Against Government. https://weetracker.com/2024/07/05/ai-use-in-kenya-protests/

65 Gachie, K. (2024, 20 June). MP John Kiarie censured after claiming OccupyParliament protest photos were 'fake'. *Citizen Digital*. https://www.citizen.digital/news/mp-john-kiarie-censured-after-claiming-occupyparliament-protest-photos-were-fake-n344350

V. RIGHT TO PRIVACY, DATA PROTECTION, AND SURVEILLANCE

37. Article 31 of the Kenyan Constitution guarantees the right to privacy. Though the Data Protection Act 2019 was put in place to protect users' data, certain exceptions are provided under the law allowing monitoring of data online and surveillance by the government under broad grounds, including national security or public interest.[66] Other laws, including the Preservation of Public Security Act and the Official Secrets Act also limit the privacy of personal data of users on similar grounds. In 2021, an amendment to the Official Secrets Act was reinstated which allowed the government, through the president's cabinet secretary to require "any person who owns or controls any telecommunications apparatus used for the sending or receipt of any data to or from any place outside Kenya" to provide such data to the government.[67] The lack of safeguards on such requests, such as the need for judicial authorisation, severely impacts the right to privacy.
38. The use of surveillance technology to monitor individuals and their activities both online and offline has triggered fears of identification and persecution among Kenyan citizens. During the #RejectFinanceBill2024 protests, Safaricom, Kenya's dominant telecommunications provider, was blamed for sharing data with law enforcement agencies to facilitate surveillance and potential abduction of protestors.[68]
39. A recent study on the use of surveillance and counterterrorism measures found that Kenya has in place elaborate measures, infrastructure and mechanisms to facilitate communication interception and surveillance that have a significant impact on civic space. The study notes the role of enablers in this surveillance, for example the implementation of mass data collection programmes such as the National Integrated Identity Management System (Maisha Namba digital ID programme), mandatory SIM card registration, national CCTV systems and other social media monitoring measures.[69] These enablers, along with broad provisions allowing surveillance by government in laws such as the Prevention of Terrorism Act and the National Intelligence Service Act, combined with weak oversight of state surveillance practices, have allowed unchecked surveillance by agencies with little accountability. There are also documented instances of the use of such surveillance to target human rights defenders.[70]

66 Privacy International. (2020). *Analysis of Kenya's Data Protection Act, 2019*. https://privacyinternational.org/sites/default/files/2020-02/Analysis%2....

67 http://www.parliament.go.ke/index.php/node/12423

68 ARTICLE 19. (2024, 28 June). Kenya: Guarantee internet access and stop surveillance of protestors. https://www.article19.org/resources/kenya-guarantee-internet-access-and-stop-surveillance-of-protesters/

69 Kapiyo, V. (2024). Op. cit.

70 Ibid.

VI. TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE AGAINST WOMEN PUBLIC FIGURES, INCLUDING HUMAN RIGHTS DEFENDERS

40. Technology-facilitated gender-based violence (TFGBV)[71] – such as cyberstalking, online harassment and doxxing, for example – encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms and email. TFGBV has the same roots as other forms of gender-based violence and is part of the same continuum. Online and offline gender-based violence do not happen in vacuums separate from each other, as women and gender-diverse people's lives online intersect frequently and in various complex ways with other areas of their lives, and violence in any one domain can often produce harm across other domains.[72]
41. KICTANet's research drawing respondents from both urban and rural areas indicates that 54% of the respondents who took part in the survey had experienced TFGBV.[73] Women are disproportionately affected by online violence as compared to their male counterparts. Women public figures such as women human rights defenders (WHRDs), women politicians, journalists and social media influencers are even more likely to be affected by TFGBV. Prevalent forms of TFGBV in Kenya include trolling, cyberbullying, cyber harassment, non-consensual sharing of intimate images, doxxing, body shaming, and gendered disinformation and misinformation among other forms of TFGBV. Facebook and WhatsApp recorded the highest percentages of prevalence of TFGBV with rates of 69.4% and 55.6% respectively.[74]
42. In addition, women politicians in Kenya have faced high levels of violence online, particularly in the run-up to elections. According to the report *Byte Bullies*, during the 2022 general elections in Kenya, 55% of women candidates faced some form of online violence, including sexual violence, trolling, hate speech or disinformation, as compared to 35.4% of male candidates.[75] This led to a chilling effect on free speech, with seven of the 29 candidates being interviewed for the report noting that they avoided using social media during the elections to avoid such abuse.[76] Earlier studies have found that after experiencing online violence, politically active women were less willing to continue engaging on social media, with 20% of Kenyan respondents pausing their social media activity in response.[77]

---

71 In this submission, we primarily use the term "technology-facilitated gender-based violence" (TFGBV), while many other terms, such as "online gender-based violence" or OGBV, are in use in international human rights spaces. Since our early research in this area, we have understood that technology-related GBV includes a broader scope of harms to be addressed, including violence in so-called "offline" or on-ground lives facilitated by technology, rather than just violence that happens in an online space.

72 Association for Progressive Communications. (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*. https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf; Association for Progressive Communications. (2023). *Feminist Principles of the Internet: Advocacy brief on violence*. https://genderit.org/FPI-paper-on-violence

73 Wamunyu, W., Jowi, F., & Kimweli, P. (2023). *Unmasking the Trolls: Research on Online Gender-based Violence in Kenya*. KICTANet. https://www.kictanet.or.ke/mdocs-posts/unmasking-the-trolls-research-on-online-gender-based-violence-in-kenya

74 Ibid.

75 Kakande, A., et al. (2023). *Byte Bullies*: A Report on Online Violence Against Women in the 2022 Kenya General Elections. Pollicy. https://pollicy.org/projects/byte-bullies/

76 Ibid.

77 Kakande, A., et al. (2021). *Amplified Abuse: Report on Online Violence against Women in the 2021 Uganda General Election*. Pollicy. https://pollicy.org/wp-content/uploads/2022/08/Amplified-Abuse-Report-on-online-violence-Against-women-in-the-2021-general-elections.pdf

43. However, existing legal statutes in Kenya do not adequately address TFGBV.[78] Though provisions of the Penal Code relating to incitement to violence, intimidation, harm, etc. could be used to tackle TFGBV, the Penal Code does not explicitly state this nor is it clear the extent to which these offences apply to the digital sphere. Circulation of "obscene" photographs is prohibited by Article 181 of the Penal Code and the Cybercrimes Act prohibits the digital transfer or publication of "intimate or obscene" images. Definitions are not provided for obscene or intimate in either statute, and the court has held that what constitutes "obscene" or "intimate" is to be judged on a case-by-case basis. The Sexual Offences Act prohibits sexual harassment, but this crime is narrowly defined to apply only in situations of authority imbalances, such as in the workplace. Furthermore, it is unclear whether this applies to online conduct as well.[79]
44. Additional barriers to combating TFGBV include the use of local languages to perpetuate TFGBV, and gaps in capacity of legislators, law enforcement, judicial officers, prosecutors, lawyers, probation officers and psychosocial support service providers in understanding the forms of TFGBV and the mechanisms through which it is carried out. There is also a need for social media platforms to be more responsive and accountable while addressing complaints of TFGBV, including investing in content moderators who are aware of the local contexts and have knowledge of local languages, and improving effectiveness and timeliness of response to TFGBV reports.

78 Nwaodike, C., & Naidoo, N. (2020). *Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks in Ethiopia, Kenya, Senegal, South Africa and Uganda*. Internews & Pollicy. https://ogbv.pollicy.org/legal_analysis.pdf

79 Ibid.

VII. RECOMMENDATIONS

45. We recommend that the government of Kenya take the following measures to uphold human rights in the digital context:

Digital access and inclusion

- Invest in infrastructure to extend broadband internet access to rural areas, including through partnerships with private sector providers and community-based networks.
- Offer targeted training programmes for adults, especially women, to equip them with the necessary digital skills for employment and participation in society. Implement mentorship programmes to increase the number of girls taking up ICT related courses in school.
- Sustain efforts to create enabling policy and regulatory environments for the development and sustainability of community-led networks. This includes support for community-driven networks so they can empower local stakeholders to build and manage their own infrastructure, ensuring that services are relevant to their specific needs; adopting appropriate spectrum management frameworks for small social-purpose operators, creating simple, affordable licensing and making public funding available for them and other small-scale networks, particularly through the effective use of universal service funds; supporting civic initiatives in small-scale infrastructure, providing training and capacity building for meaningful connectivity and content creation, offering tax incentives and providing access to financing through microfinance institutions and other hybrid funding mechanisms and business models.
- Implement subsidy programmes or partnerships with service providers to reduce costs for low-income households.
- Conduct regular assessments of connectivity availability and usage patterns to identify underserved areas and inform targeted interventions.
- Ensure that digital access is inclusive and equitable for all; and address barriers to access technology and the internet for marginalised communities, including rural communities, women and persons with disabilities. For this, the government should establish institutionalised bottom-up participation and multistakeholder decision-making processes to promote inclusive participation of communities in policy making concerning access and digital inclusion.

Freedom of expression online

- Undertake a comprehensive review of laws hindering civic space, spearheaded by Parliament, engaging stakeholders to enact reforms aligning with constitutional principles. Active citizenship, advocacy and judicial oversight remain crucial in upholding freedom of expression as a cornerstone of democratic governance in Kenya.
- Amend the Cybercrimes Act to ensure that all provisions comply with international human rights standards relating to free speech and expression; and remove all together provisions criminalising online speech contained in Sections 22, 23 and 27 of the Cybercrimes Act.
- Withdraw all cases against individuals facing harassment, intimidation and prosecution from state authorities for legitimate expression and dissent against the government.

- Promote healthy information systems that include robust access to public information; plural, accessible and diverse media contexts; independent journalism; and the possibility of expressing ideas safely to counter disinformation.[80]
- This includes encouraging social media platforms to take proactive measures to address disinformation and provide transparency on their algorithms and content moderation policies. Companies' content moderation processes (not just in how they respond to requests for takedowns, but throughout the entirety of their operations) should be guided by, among others, the principles of accountability, equality and non-discrimination, participation and inclusion, transparency, empowerment, sustainability and non-arbitrariness.[81]
- Refrain from shutting down the internet, including the blocking of particular services or applications, and make a state pledge to refrain from imposing any unlawful restrictions on internet access and telecommunication in the future, particularly in elections and protests.[82]

Right to privacy and data protection

- Refrain from using cybersecurity-related laws, policies and practices as a pretext to violate human rights and fundamental freedoms. Rather than balancing rights against security, cybersecurity-related policies must provide security in a way that reinforces human rights.[83] Amend regulatory provisions, including in the Official Secrets Act, Preservation of Public Security Act, Data Protection Act, Prevention of Terrorism Act, and the National Intelligence Service Act which permit state surveillance of online content without adequate safeguards.
- Guarantee adequate and independent oversight mechanisms which operate on principles of transparency and accountability, provide redress mechanisms to victims, and control state surveillance practices to ensure they are limited and proportional in accordance with international human rights standards.
- Encourage companies operating in Kenya to implement robust cybersecurity measures to protect personal data and prevent cyberattacks, in line with the government's obligations under the UN Guiding Principles on Business and Human Rights.

Technology-facilitated gender-based violence against women public figures, including human rights defenders

- Adopt measures and policies to prohibit, investigate and prosecute TFGBV. Ensure existing laws on gender-based violence, including the Cybercrimes Act, include aspects of TFGBV, and engage with specialists in TFGBV, including civil society organisations, survivors and academics for such law reform.
- All legislative responses to tackle this issue should be in line with international human rights standards. Legal frameworks should adequately protect women's freedom of expression, privacy and freedom from violence. Any restrictions to freedom of expression as a response to TFGBV must be necessary and proportionate, should not be overly broad or vague in terms of what speech is restricted, and should not over-penalise.

---

80 Association for Progressive Communications. (2021). *APC policy explainer: Disinformation*. https://www.apc.org/en/pubs/apc-policy-explainer-disinformation

81 Ibid.

82 Voulé, C. N. (2021). *Ending Internet Shutdowns: A path forward. Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*. https://digitallibrary.un.org/record/3929056?v=%5B%27pdf%27%5D&ln=en

83 Association for Progressive Communications. (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity

- Provide redress and reparation as an effective, efficient and meaningful way of aiding victims of TFGBV and ensuring that justice is achieved. Such measures should include forms of restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic, material, individual and collective, depending on the circumstances and the preferences of the victim.
- Regularly train judiciary, lawyers, police and law enforcement officials and frontline workers to ensure their ability to investigate and prosecute perpetrators, and foster public trust in obtaining justice for cases of TFGBV, in conjunction with broader sensitisation on addressing gender-based violence.
- Ensure that online platforms comply with their responsibilities under the UN Guiding Principles on Business and Human Rights. Develop appropriate and effective mechanisms of accountability for social media platforms and other technology companies focused on ensuring company transparency and remediation to ensure that hate speech and gender-based violence are addressed on their platforms, there is appropriate response to such instances, and safeguards and redressal mechanisms are available for those affected.
- Promote the development of TFGBV lexicons in different local languages to be used in training AI algorithms and individuals for effective content moderation to curb TFGBV.
- Proactively facilitate collaboration between various stakeholders, including technology companies, women's rights organisations, researchers and civil society, to strengthen policy making and implementation aimed at preventing and addressing TFGBV.
- Conduct a comprehensive review of domestic laws and regulations which impact access to justice. Such laws include the Evidence Act which needs to incorporate a clear and progressive direction regarding potential evidentiary and procedural issues such as chain of custody and the standards of admissibility issues related to technology-facilitated violence.