# ANALYSIS OF INTERNET SHUTDOWNS AND GOVERNANCE FRAMEWORKS IN KENYA


International Commission of Jurists
KENYAN SECTION | Since 1959

**Published by**
The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O Box 59743 - 00200, Nairobi, Kenya
Tel: +254-20-2084836/8|+254 720 491549
Email: info@icj-kenya.org
Website: www.icj-kenya.org


**Design and Layout:**
Ndolo Anderson
Lead Graphics Designer & illustrator - ICJ Kenya

## Acknowledgement

This publication, *Strengthening Legal Protections for Freedom of Expression through Digital Rights: A Critical Analysis of Internet Shutdowns and Governance Frameworks in Kenya,* is the result of collective dedication and collaboration driven by the passion to safeguard digital civic space in Kenya.

We extend our deepest gratitude to the Digital Rights portfolio at ICJ Kenya, ably managed by **Demas Kiprono,** whose stewardship and unwavering commitment throughout the project ensured its successful delivery. Special thanks to **Jaika Charles,** the Project Lead and Editor, whose visionary leadership from the inception of the research through topic formulation, coordination, and meticulous editorial guidance was instrumental in shaping the final output. Their tireless efforts and collaborative spirit made this research a true success.

Our heartfelt appreciation goes to **Ephraim Kenyanito** and his team for their exceptional research, critical analysis, and intellectual rigor that form the backbone of this publication.

We also thank **Open Society Foundations (OSF)** for their generous support in funding this project. The valuable contributions from our esteemed digital rights partners, **Article 19** and the **Bloggers Association of Kenya (BAKE),** enriched the research with practical insights and grounded perspectives on internet governance and freedom of expression in Kenya.

This publication stands as a testament to what is possible through collaboration, expertise, and a shared commitment to promoting and protecting digital rights for all.

Signed,

Eric Mukoya
Executive Director
ICJ Kenya.

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Kenya's rapid digital transformation, fueled by initiatives like the Digital Superhighway Programme, has positioned the Internet as a vital tool for economic growth, social inclusion, and political participation. Yet, this potential is increasingly undermined by recurrent Internet shutdowns, legal ambiguities, and a lack of accountability in governance frameworks. This report focusses on Kenya's and Africa's digital landscape for over a decade. "This study is framed" through the lens of preserving digital civic space. In this online arena, citizens exercise their rights to expression, information, and assembly. This report critically analyses Kenya's legal frameworks governing Internet freedom, explicitly focusing on shutdowns during politically sensitive periods like the 2024 #RejectFinanceBill protests. It proposes actionable reforms to align with international human rights standards.

The analysis reveals a troubling pattern: Kenya's constitutional guarantees under Articles 33, 34, and 35—freedom of expression, media freedom, and access to information—are eroded by vague provisions in laws like the Computer Misuse and Cybercrimes Act (2018) and the Kenya Information and Communications Act (KICA). These statutes enable government-ordered shutdowns, often justified by nebulous "national security" claims, with minimal transparency or judicial oversight. The Communications Authority of Kenya (CAK), tasked with regulating telecommunications, lacks independence from executive influence. At the same time, telecom providers like Safaricom and Airtel[1] allegedly follow shutdown directives, exacerbating socio-economic harms, evidenced by a $6.3 million daily GDP loss during the 2024 protests. Proposed legislation, such as the 2024 Cybercrimes Amendment Bill, risks further entrenching these threats by broadening state powers over digital content.

In context, the Bill grants authorities broader authority to block websites and online platforms deemed to disseminate "harmful content," a term that remains vaguely defined and open to abuse. This builds on existing loopholes in the 2018 Act, such as Section 22, which criminalises the publication of "false information" without clear definitions, allowing for subjective enforcement.

Compared to existing legal loopholes, the 2024 Bill introduces even broader discretionary powers without addressing the lack of safeguards for proportionality, necessity, and transparency. For instance, it does not require judicial approval for website blocking or data interception, nor does it establish precise mechanisms for redress for individuals whose rights are violated. This represents a significant regression in Kenya's commitment to upholding constitutional and international human rights standards, such as those outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Case studies, including the 2017 Kenyan election disruptions and Uganda's 2021 blackout, underscore the regional fragility of digital rights, while comparative lessons from India's judicial oversight and South Africa's constitutional protections highlight Kenya's regulatory deficits. Key gaps include the absence of specific shutdown laws, limited oversight mechanisms, and disproportionate impacts on vulnerable groups like rural women and small businesses.

These findings are grounded in a mixed methodology—legal analysis and case studies. To safeguard Kenya's digital civic space, the researchers recommend: (1) amending vague legal provisions (e.g., Section 22, 23 and 27 of the Cybercrimes Act) to align with ICCPR standards; (2) enacting legislation mandating judicial approval for shutdowns; (3) enhancing CAK's autonomy from executive overreach; (4) requiring telecoms to publish transparency reports on government requests; and (5) establishing compensation mechanisms for shutdown-affected users in line with the UNHRC's emphasis on access to remedies for human rights violations.

These reforms aim to enhance transparency, accountability, and legal protections, aligning with ICJ Kenya's mission to strengthen Internet freedom and Kenya's obligations under international human rights frameworks. Kenya stands at a crossroads: without urgent action, its digital promise risks becoming a tool of repression rather than empowerment. By adopting these measures, Kenya can align itself with global best practices and ensure its digital space remains a platform for democratic participation, innovation, and human rights.

[1] 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

# INTRODUCTION

## Background

The history of Internet shutdowns in Kenya can be traced back to the 2017 general elections, when the government directed telecommunications providers to block access to social media platforms and messaging services, citing concerns over the spread of hate speech and incitement to violence. Despite clear guidance under the Constitution of Kenya 2010 and various court interpretations; the government has continued to impose restrictions on Internet access during politically sensitive periods, such as the 2022 general elections, raising concerns about the misuse of laws like Section 12 of the National Cohesion and Integration Act and Section 56 of the Cybercrimes Act to justify such actions.

Internet freedom and digital rights are critical components of modern democratic societies, enabling individuals to access information, express opinions, and participate in civic activities. In Kenya, the importance of these rights is underscored by the country's rapid digital transformation and the increasing reliance on Internet connectivity for economic, social, and political activities. Through Articles 33, 34, and 35, the Kenyan Constitution guarantees freedom of expression, media freedom, and access to information, aligning with international frameworks such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Initiatives like the Digital Superhighway Programme, a World Bank-backed project aimed at expanding Internet access nationwide, have significantly shaped Kenya's digital landscape. These efforts have facilitated better connectivity and digital inclusion, contributing to economic growth and social development. However, the benefits of digitalisation are contingent upon the protection of Internet freedom and digital rights. Without these protections, the potential of the Internet as a tool for empowerment and development is severely undermined.

Despite constitutional and international protections, Kenya has experienced recurrent Internet shutdowns and other forms of censorship, particularly during politically sensitive periods such as protests and elections. These actions pose significant challenges to the free flow of information and the exercise of digital rights, raising concerns about the country's commitment to upholding these fundamental freedoms.

## Problem Statement

The primary challenges to Internet freedom in Kenya stem from legal ambiguities, government interference, and private sector complicity. The Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) under Sections 22 and 23 contain provisions that enable arbitrary arrests and unchecked surveillance, undermining the protections guaranteed by the Constitution. In addition, there is the provision on prevention of "hate speech" and "incitement" under Section 12 of the National Cohesion and Integrity Act. These laws allow for broad and vague interpretations that can be used to justify Internet shutdowns and other restrictive measures. The 2018 arrest and prosecution of Blogger, Cyprian Nyakundi, represents many of the failed and misused attempts by the government to limit the digital rights of citizens, which has a resultant effect of discouraging citizens from engaging in political discourse on digital platforms.

Government interference is evident through actions such as Internet shutdowns during protests and elections. The Communications Authority of Kenya has been implicated in issuing directives for shutdowns, often citing national security concerns. These shutdowns have significant socio-economic impacts, disrupting communication, business operations, and access to information. For instance, during the June 2024 #RejectFinanceBill2024 protests, the government ordered an Internet shutdown that lasted several days, causing daily GDP losses of $6.3 million and disproportionately affecting rural women and small businesses.

The UN General Assembly Resolution 78/213 calls for respect for human rights in the operation, use, and regulation of all digital technologies and provides redress and remedies for all abuses caused by, contributed to, or that may be directly linked to[2].

[2] UNGA Res 78/213 (22 December 2023) UN Doc A/RES/78/213

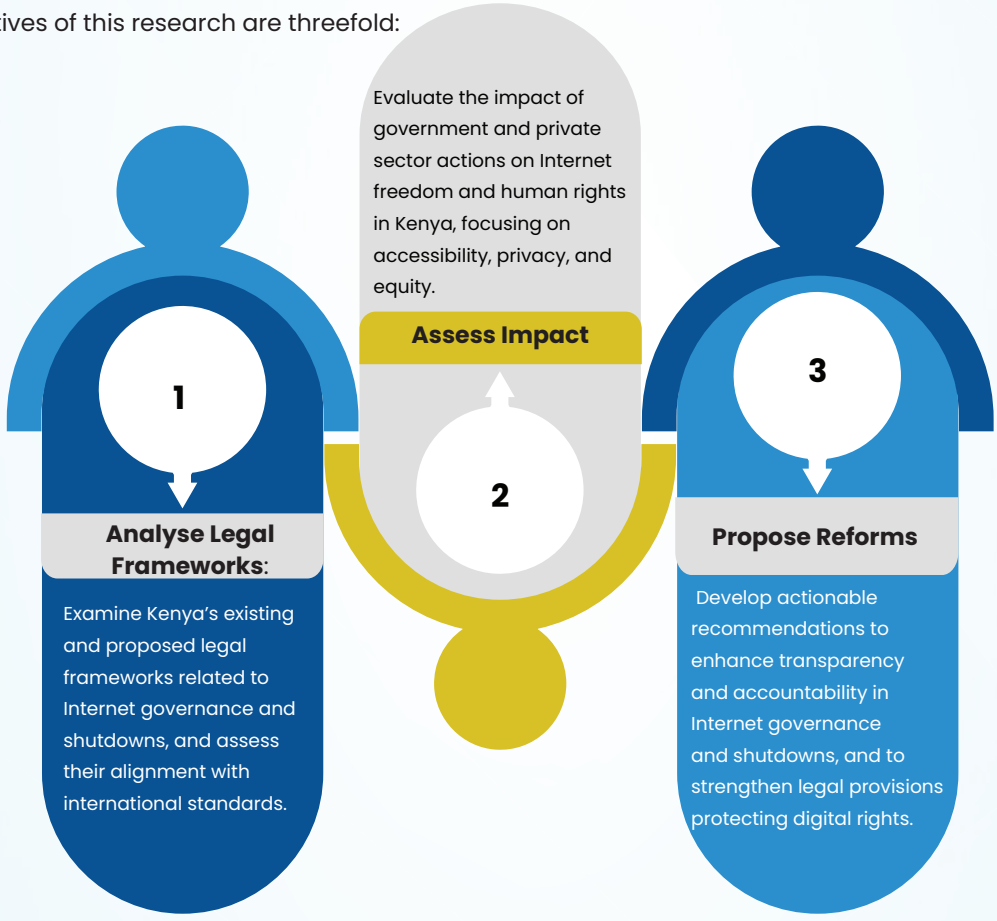
Private sector complicity further exacerbates these challenges[3]. Telecom providers like Safaricom and Airtel[4] have allegedly complied with government directives for Internet shutdowns, raising concerns about transparency and accountability. These actions highlight the need for stronger regulatory frameworks to ensure that companies uphold human rights standards and resist government overreach.

Specifically, Kenya's obligations under the UN Guiding Principles on Business and Human Rights under Pillar 2 require corporate businesses to undertake ongoing human rights due diligence to identify, prevent and mitigate human rights abuses. Fundamentally, companies should enable remediation mechanisms for the negative impacts they have caused or contributed to.[5]

In the same vein, ARTICLE 19 recommends that operators could achieve more for human rights by being more transparent about issues that affect human rights.[6] In Kenya, transparency could entail disclosure to consumers on information with which they can distinguish between typical Internet glitches and government-sanctioned disruptions.[7] Additionally, there is a critical need for explicit legal provisions that mandate corporate resistance to overreaching government orders, ensuring that companies prioritise human rights over compliance with unconstitutional actions.

## Research Objectives

The objectives of this research are threefold:




[3] Freedom House, 'Kenya: Freedom on the Net 2024 Country Report' (Freedom House 2024)<https://freedomhouse.org/country/kenya/freedom-net/2024> accessed 22 February 2025

[4] 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

[5] John Ruggie, 'Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises' (21 March 2011) UN Doc A/HRC/17/31, annex ('Guiding Principles on Business and Human Rights')

[6] ARTICLE 19, 'Getting connected: Freedom of expression, telcos and ISPs' (June 2017) <https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf> accessed 7 April 2025

[7] For instance, Ugandan President responded to media questions about the shutdown order inFebruary 2016. BBC News, 'Uganda election: Facebook and WhatsApp blocked' (18 February 2016) <http://www.bbc.com/news/world-africa-35601220> accessed 18 March 2025

## Scope of the Research

This research focuses on the following key areas:

- **Legal Frameworks:** A comprehensive analysis of existing laws, such as the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and proposed legislative frameworks. The analysis will include a comparative study of best practices from other jurisdictions, such as India and South Africa, to identify gaps and areas for improvement.

- **Transparency and Accountability:** Examining the mechanisms to ensure transparency and accountability in government directives and private sector compliance. This includes assessing the role of the Communications Authority and telecom providers in implementing Internet shutdowns and other restrictive measures.

- **Human Rights Impact:** This evaluation of the socio-economic and human rights implications of Internet shutdowns focuses on vulnerable populations such as rural women and small businesses. It includes analysing the impact on accessibility, privacy, and equity.

## Legal and Regulatory Framework.

### 1. Constitution of Kenya 2010.

The Constitution of Kenya, 2010, offers a strong legal foundation for Internet freedom, safeguarding key rights such as freedom of expression, access to information, privacy, and media independence rights that are increasingly important in the digital era. Article 33 guarantees freedom of expression, including the right to seek, receive, and impart information[8]. This protection extends to online platforms, enabling individuals to express their views, engage in discussions, and share information without undue restrictions. However, this freedom is not absolute; the Constitution permits limitations [9]based on considerations like hate speech, incitement to violence, and defamation.

Equally important, Article 35[10] enshrines the right to access information, obliging the government to facilitate public access to official information. This provision promotes transparency and accountability, ensuring citizens can request and access information affecting their interests. However, challenges persist, such as the government's reluctance to disclose sensitive information and instances where online content is restricted. This creates a gap between the constitutional promise of transparency and the practical limitations on access to information, especially in the digital space.

It follows that theories surrounding digital authoritarianism suggest that governments may employ Internet shutdowns as tools to control information and suppress dissent under the guise of maintaining national security and public order.[11] This undoubtedly contravenes established international human rights norms, despite the insistence of offending governments to uphold their "sovereign authority" to counter threats to public order.[12] A pertinent example would be the Internet shutdown witnessed in the recently dubbed #RejectFinanceBill2024 protest, where government restriction was seen as a suggestion to control the flow of information,[13] which was key to the protest essentially gaining traction over social media.

---

8 Constitution of Kenya 2010.

9 Constitution of Kenya 2010.

10 Constitution of Kenya 2010.

11 K V Bhatia and others. 'Protests, Internet shutdowns, and disinformation in a transitioning state.' Media, Culture & Society, 45 (2023): 1101 – 1118. <https://doi.org/10.1177/01634437231155568/> accessed 18 March 2025

12 Steven Feldstein, 'Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?' (Carnegie Endowment for International Peace, March 2022) <https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en/> accessed 18 March 2025

13 APC, 'Digital protests, access and freedoms in Kenya' (18 July 2024) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 18 March 2025

Privacy is another critical right under the Constitution, as outlined in Article 31[14]. This right protects individuals from unwarranted surveillance and interference with their private affairs. This provision is critical on the Internet, given the rise of digital surveillance, data collection, and online tracking.

Further reinforcing Internet freedom, Article 32[15] guarantees freedom of conscience, religion, belief, and opinion, ensuring that individuals can freely express their beliefs and opinions online. The Internet has become a primary political, social, and religious discourse space. However, the government has occasionally imposed restrictions on online speech, often under the guise of national security or the fight against radicalisation, hate speech, and misinformation[16]. These restrictions sometimes undermine the broader constitutional goal of promoting free expression, mainly when used selectively to stifle dissent.

Article 34[17] guarantees freedom of the media, which is integral to ensuring a free and open Internet. In its digital form, the media plays a central role in providing information, educating the public, and facilitating debate on essential issues. Yet, there have been increasing cases of censorship, media shutdowns, and content moderation by both the government and private platforms[18]. While some of these actions are justified by concerns over hate speech or national security, they can be used to suppress dissenting voices, raising questions about the balance between regulation and freedom. The independence of digital media is essential for maintaining a pluralistic and democratic society[19].

Article 38 supports political participation, including the right to engage in political activities and expression online. The Internet has become a crucial tool for political mobilization, enabling citizens to engage in political discourse, campaign, and advocate for change. However, during election periods, attempts have been made to regulate digital campaigning, restrict political content, and combat misinformation. These measures often conflict with the right to free political expression, leading to debates over regulatory limits and digital rights protection during such critical periods.

Finally, Article 21 requires the state to respect, protect, promote, and fulfill human rights. This obligation mandates that the government ensure policies and laws enacted do not undermine fundamental rights. The most critical fundamental rights in the context of Internet shutdowns pertain to the denial of the citizen's right to access information and freedom of expression, as has been established by many court precedents. Regarding contextualisation, Section 29, KICA was among the few established laws that were key in prosecuting bloggers. However, it was challenged in the case of ***Geoffrey Andare v Attorney General & 2 others***, which led to the section being declared unconstitutional.[20] This speaks to the government's role in ensuring its policies and laws do not undermine fundamental rights and the courts' role in interpreting such rights.

In the larger African context, the African Court, while dealing with the application brought against the State of Guinea,[21] noted that the right to information aims to enable citizens to participate usefully in the democratic process and decisions concerning their future. It held that the right to information is an extension of freedom of the press and freedom of expression and that any unjustified measure that suspends or restricts free access to information constitutes a violation of the right to information. As such, the government's actions in interrupting access to the Internet without justification constituted a violation of the right to information.

---

14 Constitution of Kenya 2010.

15 Constitution of Kenya 2010.

16 CIPIT, 'Technology-Facilitated Rights and Digital Authoritarianism: Examining the Recent Internet Shutdown in Kenya' *(Centre for Intellectual Property and Information Technology Law,* 9 August 2024) <https://cipit.org/technology-facilitated-rights-and-digital-authoritarianism-examining-the-recent-internet-shutdown-in-kenya/> accessed 15 February 2025.

17 Constitution of Kenya 2010.

18 Pulselive Kenya, '6 Media Houses Warned over Coverage of Azimio Mass Action Protest' (29 July 2024) <https://www.pulselive.co.ke/articles/news/local/citizen-tv-ntv-k24-kbc-tv47-and-ebru-tv-warned-over-coverage-of-azimio-protest-20240729085143951O1> accessed 15 February 2025

19 J ack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society', Popular Culture and Law (Routledge 2017).

20 *Geoffrey Andare v Attorney General & 2 others* [2016] eKLR (Kenya)

21 *Association des Blogueurs de Guinee (ABLOGUI) and Others v State of Guinea* [2023] ECOWASCJ 1 (ECOWAS)

These constitutional provisions form a comprehensive framework for protecting Internet freedom in Kenya. While they provide a strong legal basis for protecting digital rights, challenges remain in their practical implementation, especially as digital technology evolves. Notably, the absence of explicit constitutional provisions or specific laws governing Internet shutdowns in Kenya creates a significant gap in the legal framework, leaving room for arbitrary actions that may undermine digital rights.

Continued judicial oversight, legal reforms, and advocacy for digital rights will be necessary to ensure that Kenya upholds its constitutional promise of a free and open Internet. Furthermore, the Courts' crucial role in interpreting digital rights in past cases, such as addressing Internet access as a fundamental right, sets a precedent as a judicial trend aimed at guiding future legal reforms. Balancing security concerns, regulation, and individual freedoms is key to ensuring that the Internet remains a space for democratic participation, expression, and access to information.

## 2. Computer Misuse & Cybercrimes Act, 2018

The Computer Misuse and Cybercrimes Act[22] is a critical piece of Kenya legislation addressing cybercrime and online conduct issues. While the Act aims to regulate online activities to prevent harm, its provisions have sparked concerns over Internet freedom, particularly with respect to free expression, privacy, and access to information. Below is an analysis of specific sections of the Act that relate to Internet freedom:

Section 22 criminalises the publication of false information, particularly when it is likely to cause fear, harm, or violence. This provision has significant implications for Internet freedom, as it grants authorities the power to target individuals who share content deemed false or misleading. While this provision addresses issues such as misinformation and fake news, it raises concerns about the potential for government overreach, where legitimate opinions or political commentary could be prosecuted as "false information." The subjective nature of what constitutes false information can stifle free speech and curb the diversity of voices in online spaces, especially if applied in a manner that targets political dissent or controversial opinions.

Section 23 criminalises publication of false information calculated to cause panic, chaos or violence, or likely to discredit the reputation of a person. While this section intends to protect public order, national security and rights and reputations of others, it invents its own limitations to freedom of expression that are inconsistent with Article 33 (2), such as propaganda for war, incitement to violence and advocacy for hatred. Regarding protecting the reputations of others, the law sneaks back criminal defamation, which had been declared unconstitutional by the High Court in 2017.

Section 27 seeks to protect individuals from cyber harassment. However, it contains broad terms such as criminalising content that causes "apprehension" or fear of violence to them or damage or loss to that person's property; or "detrimentally affects that person"; or "grossly offensive nature". These may offend the principle that limitations for freedom of expression must be clear and concise.. The Act's[23] provisions could be used to prosecute individuals for online speech that is critical, controversial, or confrontational, even if it does not constitute harassment. The fear of being charged under this section may discourage people from engaging in critical discourse or expressing dissenting opinions, thus potentially infringing on freedom of expression.

In the Kenyan context, the online campaign dubbed, "Tumtumie Salamu" was a representation of such instances, where the publication of public servants contacts across social media platforms was met with threats of prosecution and launch of complaints from the Office of the Data Protection over violation of the right to privacy as a protection accorded under the Act.

While the government runs along with maintaining public order and national security, a line has to be drawn between a State's sovereign authority and accountability measures. Since its enactment, persons who have been arrested for the dissemination of false information have been charged under both sections 22 and 23 of the CMCA.

---

22 Computer Misuse and Cybercrimes Act 2018 (Kenya)

23 Computer Misuse and Cybercrimes Act 2018 (Kenya)

The Act has been weaponised as a tool to combat dissent. Bloggers and activists such as Edgar Obare[24] and Mutemi wa Kiama[25] are some of those who have been arraigned in court over violation of this law after threats and intimidation from unknown third parties. Activists have also been threatened with arrest and other consequences for speaking out on issues touching on police brutality. Others have even had their laptops and other equipment confiscated.[26]

Section 24 criminalises unauthorised access to information, which includes hacking or accessing someone else's computer systems without permission. While this provision is essential for protecting individuals' and organisations' data privacy and security, it has raised concerns regarding protecting journalists, whistleblowers, and activists. In some cases, the law could be misused to target individuals or groups attempting to expose corruption or wrongdoing[27], as unauthorised access to certain information might be perceived as a criminal act. This provision could be seen as limiting access to information, particularly when uncovering abuses of power or holding authorities accountable, potentially infringing upon the public's right to access important information.

Section 26 criminalises identity theft and impersonation, particularly using someone else's personal information for fraud. While protecting individuals from identity theft is crucial for online safety, this section could have implications for digital rights if misapplied. For instance, activists or whistleblowers who attempt to expose government corruption or abuse may be at risk of being accused of impersonating officials or unauthorised access. Furthermore, the law could be used to suppress digital activism or independent journalism if authorities target individuals who engage in online campaigns using pseudonyms or anonymous profiles, undermining the right to freedom of expression and participation.

Section 27 defines and criminalises cyberterrorism, which involves the use of technology to promote terrorism or extremist acts. While the Act aims to protect national security by preventing cyberattacks that threaten the country's infrastructure, there is concern that this section may be used to justify broad surveillance or censorship of online content. Under the guise of national security, this section could be misused to restrict political speech, suppress activism, or censor online discussions critical of government policies. The potential for the law to be applied to curtail legitimate political engagement, protests, or free speech is a significant challenge to Internet freedom.

Section 34 allows for the interception of communications under specific conditions, particularly to investigate crimes. While the goal of preventing cybercrimes is essential, the provisions of this section have raised significant concerns regarding privacy and surveillance. The ability of authorities to monitor online communications can lead to the infringement of individuals' right to privacy, particularly if such powers are exercised indiscriminately or without proper judicial oversight[28]. The risk of over-surveillance is heightened in the digital age, where governments could monitor political dissidents, journalists, or activists, thereby chilling free expression and curtailing the right to privacy.

Section 37 grants authorities the power to arrest individuals suspected of committing offenses under the Act without a warrant, particularly in cases involving cybercrimes. While this provision is designed to enhance law enforcement's ability to quickly respond to cyber threats, it raises concerns about the potential for arbitrary arrests and the abuse of power.

---

24 Directorate of Criminal Investigations (@dci_kenya), 'Statement on arrest of Edgar Obare under Section 23 of Computer Misuse and Cybercrimes Act 2018' (X, 4 March 2021) <https://twitter.com/dci_kenya/status/1367512899044925442/> accessed 18 March 2025

25 ARTICLE 19, 'Kenya: Release and cease attacks on Edwin Mutemi wa Kiama' (8 April 2021) <https://www.article19.org/resources/kenya-cease-attacks-on-and-release-edwin-mutemi-wa-kiama/> accessed 18 March 2025

26 Human Rights Watch, 'Kenya: Police Threaten Activists Reporting Abuse' (4 June 2018) <https://www.hrw.org/news/2018/06/04/kenya-police-threaten-activists-reporting-abuse> accessed 22 February 2025

27 Abdulmalik Sugow and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1(1) JIPIT <https://www.researchgate.net/publication/352475154_Appraising_the_Impact_of_Kenya's_Cyber-Harassment_Law_on_the_Freedom_of_Expression> accessed 17 February 2025

28 Mugambi Laibuta, 'State surveillance: Kenyans have a right to privacy – does the government respect it?' (*The Conversation*, 29 November 2024) <https://www.polity.org.za/article/state-surveillance-kenyans-have-a-right-to-privacy-does-the-government-respect-it-2024-11-29> accessed 17 February 2025

The broad application of this section could be used to target individuals who engage in online activism, critical reporting, or political opposition[29]. If not carefully controlled, such provisions could lead to a chilling effect on free expression, as individuals may fear legal repercussions for their online activities.

Section 50 outlines the liability of Internet intermediaries, such as Internet service providers (ISPs) and social media platforms, for content hosted or transmitted through their services.

This section can affect Internet freedom, particularly when platforms are pressured to follow government requests to censor or remove content critical of the government. The potential for Internet intermediaries to act as gatekeepers, by either removing content or blocking access to websites, raises concerns about the erosion of free speech online[30]. In some instances, these platforms may be compelled to restrict online content to avoid facing legal consequences, undermining the principle of free and open access to information.

Section 56 of the Act gives the government powers to regulate and control digital content, particularly concerning national security, public order, and morality. This section raises concerns about Internet shutdowns and content filtering, particularly during political unrest, protests, or elections. The broad scope of regulation could be used to justify the shutdown of social media platforms or entire Internet services, which would infringe on citizens' rights to access information, communicate freely, and participate in democratic processes. While content regulation is necessary to address harmful or illegal online activity, it should not be used to suppress free expression or limit the flow of information.

## Data Protection Act, 2019

The Data Protection Act, 2019[31] and its regulations in Kenya contain provisions that raise significant concerns about the balance between privacy, Internet freedom, and public interest. Several controversial sections can potentially undermine individuals' privacy rights, particularly regarding indirect data collection, exemptions from consent, and the scope of data processing for law enforcement, national security, and public interest.

Section 41 of the Act outlines broad exemptions, allowing personal data to be processed without consent for national security, law enforcement, and public interest purposes. Though necessary for certain state functions, these exemptions are controversial because they could be used to justify mass surveillance and unwarranted data collection under vague justifications. The national security exemption, for instance, opens the door to invasive data collection, potentially infringing on individuals' rights to privacy and freedom of expression, especially if the criteria for "national security" are not clearly defined[32].

Section 41(2) further exempts data processing for investigating or prosecuting crimes, enabling law enforcement agencies to collect personal data without consent. While essential for crime prevention, this provision raises concerns about overreach and the potential for surveillance, mainly when such activities are conducted without oversight. Similarly, Section 41(3) allows personal data to be processed in the public interest, including activities like public health research or safety measures. However, the broad interpretation of public interest may be exploited for data collection purposes unrelated to public welfare, infringing individual privacy.

Regulation 14, which deals with the indirect collection of personal data for law enforcement or public interest, is another area of contention. This regulation permits data to be gathered without the subject's direct consent, including through third-party data collection or surveillance.

---

29 Abdulmalik Sugow and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1(1) JIPIT <https://www.researchgate.net/publication/352475154_Appraising_the_Impact_of_Kenya's_Cyber-Harassment_Law_on_the_Freedom_of_Expression> accessed 17 February 2025

30 Council of Europe (Freedom of Expression), 'The Role of Internet Intermediaries as Gatekeepers to Freedom of Expression – Conference in Vienna' (2017) <https://www.coe.int/en/web/portal/-/the-role-of-internet-intermediaries-as-gatekeepers-to-freedom-of-expression-conference-in-vienna> accessed 17 February 2025

31 Data Protection Act 2019 (Kenya)

32 Mercy Muendo, 'Kenya Plans to Place Public Security above Data Privacy. That's a Bad Idea' (The Conversation, 11 February 2019) <http://theconversation.com/kenya-plans-to-place-public-security-above-data-privacy-thats-a-bad-idea-111099> accessed 17 February 2025

While necessary for criminal investigations, the regulation could be misused to conduct broad, intrusive monitoring of individuals, undermining the principle of informed consent and leaving people unaware that their data is being processed.

Moreover, the guise of national security may be used to justify Internet shutdowns. Authorities might argue that indirect data collection alone is insufficient to address imminent threats such as organised crime, thus necessitating a complete shutdown of Internet services to prevent the spread of harmful content or coordination of illegal activities. Without clear legal safeguards and judicial oversight, the broad language of Regulation 14 risks being exploited to legitimise excessive measures that undermine digital rights under the pretext of national security.

## Kenya Information & Communication Act, 1998

The Kenya Information and Communications Act (KICA) regulates communications, including the Internet, broadcasting, and telecommunication services in Kenya. While designed to promote efficient communication and broadcasting services, specific provisions of KICA[33] raise concerns regarding Internet freedom and privacy.

Section 84 on retention of communication data mandates that telecommunications service providers retain user communication data, including Internet browsing history, for up to two years to assist in law enforcement investigations. While aimed at combating crime, the lack of clear guidelines for data protection and the potential for unauthorised access to this retained data heighten concerns over privacy violations. The risk of mass surveillance is significant, and the provision lacks oversight mechanisms to ensure that the data is not misused.

Section 88 grants the Communications Authority of Kenya (CAK) the authority to monitor, regulate, and censor content transmitted over electronic communications. The broad powers provided to the CAK raise concerns about potential censorship, particularly when content critical of the government or national interests is deemed harmful. The discretion to regulate content without adequate checks and balances could suppress free expression, especially in politically sensitive contexts. The lack of oversight increases the potential for abuse and curtails the diversity of online content.

These provisions within KICA threaten Internet freedom by allowing mass surveillance and broad content control without sufficient safeguards, potentially undermining online privacy rights and freedom of expression.

## Prevention of Terrorism Act, 2012

The Prevention of Terrorism Act (POTA)[34] aims to curb terrorism activities in Kenya. While crucial for national security, several sections have raised concerns about Internet freedom and privacy, particularly regarding surveillance and data collection.

Section 26 allows law enforcement agencies to intercept communications, including Internet communications, when investigating or preventing terrorism. The broad authority granted for communication interception raises concerns over the surveillance of individuals not connected to terrorism. The lack of defined limits on the scope of surveillance may lead to widespread monitoring of online activities without adequate safeguards or oversight.

Section 29 allows authorities to collect personal data from service providers to aid terrorism-related investigations. This provision provides access to vast amounts of personal data, including communication logs and Internet usage data, which can infringe on privacy. The ability to collect data without sufficient checks and balances poses a significant risk of mass surveillance, particularly for individuals not involved in criminal activities.

[33] Kenya Information and Communications Act 1998 (Kenya)

[34] Prevention of Terrorism Act 2012 (Kenya)

## National Cohesion & Integration Act, 2008

The National Cohesion and Integration Act (NCIA)[35] promotes national unity and prevents ethnic and political violence in Kenya. However, specific provisions raise concerns about online freedom of expression and the potential for censorship.

Section 13 criminalises the use of hate speech and the incitement of violence through communication platforms, including social media. While necessary for national unity and peace, the definitions of "hate speech" and "incitement" are broad and open to subjective interpretation.

The ambiguity in these definitions could restrict legitimate political discourse or controversial opinions, potentially stifling free speech online.

An equally good example as the basis for the Internet Shutdown in 2017, as claimed by the government, was to curb the spread of hate speech, misinformation and incitement to violence. The resulting factor, however, was a limitation on digital rights, such as access to information and freedom of expression, in implementing an Internet shutdown without demonstrating that less restrictive measures were insufficient. The reliance on this section for the prosecution of bloggers has had a chilling effect, discouraging Kenyans from engaging in online discussion, particularly on sensitive topics such as politics and governance issues.

Section 13 empowers the government to monitor and control content promoting political or ethnic violence. The vague wording of "political or ethnic violence" raises concerns that it could be used to suppress free expression on politically sensitive issues. The broad discretion granted to authorities to regulate content may cause the censorship of opinions critical of government policies or controversial ethnic matters, limiting the diversity of political discourse online.

Section 62 criminalises the publication or distribution of materials that are threatening, abusive, or insulting and likely to incite ethnic hatred. While this provision aims to prevent the spread of harmful content, the lack of clear definitions for these terms leaves room for subjective interpretation and potential misuse by authorities. This section can target critics, activists, and journalists who publish controversial content online, particularly political commentary. Moreover, it does not provide sufficient protection for legitimate public debate, leading to a chilling effect on online discussions due to the fear of prosecution.

Closely related is Section 62(2), which criminalises intent to incite ethnic hatred, even if the material published did not lead to such incitement. This provision is particularly problematic because it allows authorities to prosecute individuals based on perceived intent rather than clear evidence of harm. Such an approach opens the door for arbitrary enforcement and could be used to silence online activists, bloggers, and independent media expressing dissenting views. The risk of individuals being prosecuted for sharing political or controversial opinions is high, as authorities could claim that such content was intended to incite hatred.

Another concerning provision is Section 63, which prohibits the possession, publication, or dissemination of materials that promote ethnic hatred, including digital content shared on social media. The broad and undefined scope of what constitutes "hate-related materials" raises concerns that political or dissenting opinions could easily be criminalised. Additionally, this provision makes online users and platforms liable for simply sharing or even unknowingly possessing controversial content. Given the lack of judicial oversight, enforcement could disproportionately target political opposition, human rights defenders, or minority groups, further restricting free speech online.

The National Cohesion and Integration Commission (NCIC) powers under Section 66 add another layer of concern. The NCIC is granted authority to investigate, prosecute, and recommend legal action against individuals accused of promoting ethnic hatred or incitement. However, the Commission has been criticised for political bias, raising concerns that these powers could be used selectively to target government critics while ignoring speech that supports those in power.

35 National Cohesion and Integration Act 2008 (Kenya)

Furthermore, its ability to monitor online content without clear procedural safeguards increases the risk of mass surveillance and censorship, undermining Internet freedom.

Section 67 further restricts online expression by prohibiting media houses from publishing or broadcasting content deemed "prejudicial to cohesion and integration." The vague nature of this provision makes it possible for authorities to restrict news reports, opinion pieces, or online discussions that critique the government.

Media houses, bloggers, and social media users could face penalties for publishing investigative reports on corruption, electoral fraud, or human rights violations if such content is deemed to undermine "cohesion." This provision could also justify blanket bans on social media platforms or suppress online discussions, particularly during elections or political unrest.

## Proposed legislation and its impact on free speech.

Kenya has seen several proposed laws and regulations in recent times following the #RejectFinanceBill2024 protests; this legislation touches on freedom of expression, social media regulation, and Internet shutdowns. These proposals have arisen as a disguise to balance national security, public order, and individual rights, but they have sparked debates about their potential impact on democratic freedoms. Below are some notable examples based on recent developments:

### i. Computer Misuse and Cybercrimes (Amendment) Bill, 2024

This bill seeks to amend the existing Computer Misuse and Cybercrimes Act of 2018, which governs cyber offenses in Kenya. The proposed amendments aim to expand the government's powers to address illegal online activities. It includes measures to allow authorities to close websites and applications that perform unlawful activities, such as spreading misinformation, inciting violence, or hosting harmful content. It also broadens the definitions of cyber offenses. Critics argue that the vague wording of "illegal activities" could lead to overreach, potentially stifling free speech and access to information[36]. The ability to block websites raises concerns about censorship and suppressing dissenting voices.

The bill reflects a growing push to regulate digital spaces amid concerns over misinformation and security, but it has been met with calls to ensure it doesn't undermine constitutional rights like freedom of expression enshrined in Article 33 of the Kenyan Constitution.

### ii. Kenya Information and Communications (Amendment) Bill, 2019 ("Social Media Bill")

Proposed by Malava MP Moses Injendi, this Bill aimed to introduce strict regulations on social media use in Kenya by amending the Kenya Information and Communications Act (KICA). The law would require bloggers and social media group administrators to obtain licenses from the Communications Authority of Kenya (CA). The bill also mandated that social media platforms accessible in Kenya have a physical office in the country and maintain user data for submission to the CA upon request. Further, the bill imposed obligations on users to refrain from posting certain types of content, though penalties for non-compliance were unclear.

The Bill was widely criticised for infringing on privacy, freedom of expression, and association. Human rights advocates, including Amnesty International Kenya, argued it threatened the democratic strides made in digital expression[37]. The ICT Committee of Parliament deemed it unconstitutional, citing violations of rights to speech and privacy. Due to public outcry and opposition from stakeholders like the Kenya Union of Journalists and the Bloggers Association of Kenya, the bill did not progress beyond its first reading and was effectively shelved..

[36] kictanetadmin, 'Proposal to Block Websites and Applications Threatens Kenya's Digital Ecosystem' (KICTANet Think Tank, 2 October 2024) <https://www.kictanet.or.ke/proposal-to-block-websites-and-applications-threatens-kenyas-digital-ecosystem/> accessed 23 February 2025

[37] Brian Murimi, 'Proposed Changes to Kenya's Constitution: A Look at the 2024 Amendment Bill' (Sharp Daily, 2 October 2024) <https://the-sharpdaily.com/kenya-constitutional-amendment-bill-2024/> accessed 23 February 2025

## Case Study of Internet Shutdowns and the Interconnection with Civil Space

The erosion of Internet freedom and freedom of expression in Kenya has been marked by numerous incidents involving state interference, online censorship, surveillance, and crackdowns on dissent. While the government has sometimes upheld digital access, various legal and extrajudicial measures have been used to suppress critics, silence activists, and control online discourse.

Examining specific case studies helps to illustrate how state agencies have wielded laws, technology, and security forces to intimidate and punish those exercising their rights. From Internet shutdowns and digital surveillance to arbitrary arrests and violent crackdowns on protesters, these instances highlight the fragile state of Internet freedom in Kenya and the ongoing struggle to protect digital rights in an increasingly repressive environment.

### i. Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)[38]

In 2017, the Bloggers Association of Kenya (BAKE) challenged the Computer Misuse and Cybercrimes Act, 2018, arguing that specific provisions violated the freedom of expression and Internet freedom guaranteed under Articles 33 and 34 of the Kenyan Constitution. Specifically, BAKE contested sections criminalising false publication, cyber harassment, and the misuse of telecommunication devices, claiming that these provisions were vague, overbroad, and susceptible to abuse by state authorities. The High Court initially suspended the enforcement of these contentious provisions, but subsequent rulings allowed the government to enforce most of them. This case highlights the ongoing legal battles over digital rights in Kenya, where cybercrime laws are often used to target journalists, bloggers, and activists under the guise of regulating online content.

### ii. The Arrest of Cyprian Nyakundi and Other Bloggers

Kenyan bloggers and social media commentators, particularly those publishing critical content, have frequently faced arrests and intimidation. A prominent example is Cyprian Nyakundi, a blogger known for exposing alleged corruption and misconduct among Kenya's political and business elites. Nyakundi was arrested multiple times under Section 23 of the Computer Misuse and Cybercrimes Act, which criminalises the publication of "false information." His case underscores how laws designed to combat cybercrime are often weaponised to suppress dissent and curb investigative journalism, threatening the fundamental right to freedom of expression and access to information.

### iii. The 2024 Finance Bill Protests

In mid-2024, widespread protests erupted in response to a proposed finance bill that included controversial tax hikes. These protests, organised mainly by Generation Z activists through social media, faced heavy crackdowns by security forces. At least 23 protesters were killed, and hundreds were arrested[39]. The government's heavy-handed response, including reports of abductions and intimidation, raised serious concerns about the suppression of dissent and the erosion of Internet freedom[40]. The protests also highlighted the critical role of social media in facilitating decentralised activism and how authorities responded with excessive force to stifle political dissent.

---

38 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR (Kenya)

39 Nita Bhalla, 'Why has Kenya's finance bill triggered protests?' (*Context.news*, 26 June 2024) <https://www.context.news/money-power-people/why-has-kenyas-finance-bill-triggered-public-outrage> accessed 17 February 2025

40 Nicholas Mwangi, 'Surge in Abductions of Government Critics in Kenya Sparks Mass Public Outcry' (*Peoples Dispatch*, 14 January 2025) <https://peoplesdispatch.org/2025/01/14/surge-in-abductions-of-government-critics-in-kenya-sparks-mass-public-outcry/> accessed 17 February 2025

### iv. Abduction of Kizza Besigye

In November 2024, Ugandan opposition leader and activist Kizza Besigye was abducted in Kenya and forcibly returned to Uganda[41]. Besigye was in Kenya to attend a book launch by Martha Karua, a known critic of the Kenyan government. His abduction highlights the increasing risks faced by government critics and the apparent collaboration between regional security agencies to suppress dissent. This incident is a stark reminder of the escalating challenges faced by activists and critics within the region.

### v. Abduction of Maria Sarungi Tsehai

In January 2025, a prominent Tanzanian activist and media owner, Maria Sarungi, who fled to Kenya in 2020 owing to her intense criticism of the government, was kidnapped in Kenya with concerted efforts to transport her to Tanzania.[42]

This presents the critical danger presented to online activists who dare act as critics of the government, even with Sarungi's story showing the strong determination behind her kidnappers' wanting to gain access to her phone and have access to her social media accounts unsuccessfully. This equally presents a harsh reality of day-to-day risks faced by online activists and any individuals whose expressions do not fit a positive 'government agenda' and 'security.'

## Comparative Analysis: Lessons from Other Jurisdictions

**A Case Study of India**

***Anuradha Bhasin v. Union of India and Ghulam Nabi Azad v. Union of India*** is a landmark case where the Indian Supreme Court, accepted that Article 19(1)(a) protects the right to disseminate and receive information online. Therefore, the constitutional validity of every Internet shutdown would have to be tested (at least) against the three standards ordinarily applied to test restrictions on the freedom of speech.[43] It held that suspension of Internet services is a "drastic measure" that must be considered by the state only if it is "necessary" and "unavoidable," after assessing the "existence of an alternate less intrusive remedy."

Human Rights Watch and Internet Freedom Foundation identified 127 shutdowns in the three years between the Supreme Court's *Anuradha Bhasin* judgment in January 2020 and December 31, 2022.[44] Of 28 Indian states, 18 shut down the Internet at least once in these three years. Local authorities used Internet shutdowns in 54 cases to prevent or in response to protests, 37 to prevent cheating in school examinations or exams for government jobs, 18 in response to communal violence, and 18 for other law and order concerns. This number barely included Internet shutdowns in the Union Territory of Jammu and Kashmir, where the authorities continued to shut down the Internet more than any other place in the country.

The persistence of Internet shutdowns in India, particularly in an era of 'Digital India', where the government actively promotes Internet access as a key development tool, presents significant contradictions. These disruptions interfere with essential social protection programs, such as the National Food Security Act, which provides subsidised food grains through a targeted public distribution system. Additionally, shutdowns hamper rural banking services, delay utility bill payments, and obstruct access to official documentation—all of which disproportionately impact marginalised communities.

---

41 Amnesty International, 'Uganda: Opposition Politician Charged after Abduction: Kizza Besigye' (*Amnesty International*, 26 November 2024) <https://www.amnesty.org/en/documents/afr59/8779/2024/en/> accessed 17 February 2025

42 Danai Nesta Kupemba & Ian Wafula, 'Manhandled and choked - Tanzanian activist recounts abduction' (*BBC News Online* (London), 13 January 2025) <https://www.bbc.com/news/articles/cd7dxz48e0lo/> accessed 20 February 2025

43 Hardwaj, Shrutanjaya; Nayak, Nakul; Dandamudi, Raja Venkata Krishna; Singh, Sarvjeet; and Handa, Veda (2020) "Rising Internet Shutdowns in India: A Legal Analysis," *Indian Journal of Law and Technology*: Vol. 16: Iss. 1, Article 7.<https://repository.nls.ac.in/ijlt/vol16/iss1/7/> accessed 20 February 2025

44 Human Rights Watch, 'No Internet Means No Work, No Pay, No Food' (*Human Rights Watch*, 14 June 2023) <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic#:~:text=the%20court%20said:-,Arbitrary%20Internet%20Shutdowns,once%20in%20these%20three%20years./> accessed 20 February 2025

Governments often justify Internet shutdowns by citing concerns over mob violence fueled by online misinformation. However, United Nations human rights experts in the 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations stated that even in times of civil unrest, "using communications 'kill switches' can never be justified under human rights law." The UN Human Rights Council further reinforced this stance in 2016, unequivocally condemning Internet shutdowns and urging states to "refrain from and cease such measures."

Moreover, the International Covenant on Civil and Political Rights (ICCPR)—to which India is a party—recognises Internet access as an enabler of fundamental human rights. In 2021, the UN Secretary-General emphasised the need for universal Internet access as a human right by 2030, further highlighting the incompatibility of blanket Internet shutdowns with international legal standards.

**A Case Study of South Africa**

In contrast to India, South Africa has a strong legal framework that protects Internet access as a fundamental right. The Constitution of South Africa, 1996, explicitly guarantees freedom of expression, including digital communication. Key legislations such as the Electronic Communications Act, 2005, and the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), 2002, regulate government intervention in telecommunications, ensuring that any restrictions align with constitutional safeguards. Notably, South Africa lacks specific laws permitting arbitrary Internet shutdowns.

The judiciary has consistently upheld the Internet's role in fostering democratic participation and economic growth, reinforcing that any restrictions must conform to constitutional mandates. However, while South Africa has not yet experienced large-scale Internet shutdowns, it is a growing and pernicious problem in Sub-Saharan Africa. Ordered by states to telecommunications companies, Internet shutdowns infringe on the right to freedom of expression, disrupt online services and create losses for telecoms companies. Incidents are on the rise, despite growing authoritative guidance that Internet shutdowns infringe on international human rights law.[45]

## Identified Gaps and Improvement Areas for Kenya.

A comparative analysis of legal frameworks on Internet shutdowns in India and South Africa highlights critical regulatory gaps in Kenya's approach. India, despite its controversial history of frequent shutdowns, has a formalised legal framework under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, which grants government officials the authority to order shutdowns under specific conditions.[46] In contrast, South Africa leans towards stronger constitutional protections, recognising access to the Internet as an extension of fundamental rights such as freedom of expression and access to information.[47]

Kenya, however, lacks explicit legal provisions governing Internet shutdowns, resulting in legal ambiguity, weak oversight, and a heightened risk of human rights violations. The following are key gaps and areas for improvement:

### i. Weak Constitutional Protection for Internet Access.

To prevent future Internet shutdowns, the Kenyan government must prioritise respecting and protecting constitutional and human rights, particularly freedom of expression, access to information, and peaceful assembly. These rights are fundamental and should not be compromised by Internet shutdowns.

---

45 Business and Human Rights Resource Centre, 'Internet shutdowns in Africa: Addressing the human rights responsibilities of telecoms companies' (*Business and Human Rights Resource Centre,* 10 May 2023) <https://www.business-humanrights.org/en/from-us/briefings/internet-shutdowns-in-africa-addressing-the-human-rights-responsibilities-of-telecoms-companies//>accessed 20 February 2025

46 Bailey, Rishab & Parsheera, Smriti. 'Data localisation in India: Questioning the means and ends,' (Working Papers 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18-242.html/> accessed 22 February 2025

47 Arthur Gwagwa and others, 'Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions' (2020) 26 The African Journal of Information and Communication 3 <http://dx.doi.org/10.23962/10539/30361> accessed 19 February 2025

It is also crucial for the government to commit to transparency and accountability, providing comprehensive explanations for any Internet shutdowns. Ensuring that such decisions are made transparently and with clear accountability allows the public to understand the reasons behind these significant actions.

### ii. Lack of Clear Legal Provisions regulating Internet shutdowns

Kenya has no legal framework explicitly addressing Internet shutdowns, creating a regulatory vacuum. While the Kenya Information and Communications Act (KICA), 1998, grants the Communications Authority (CA) the power to regulate telecommunications, it does not explicitly address Internet shutdowns or outline due process for imposing restrictions (KICA, 1998).

In contrast, India's legal framework provides structured, though often criticised, guidelines for implementing shutdowns, requiring formal authorisation from high-level government officials and periodic review mechanisms.[48]

Kenya should consider developing explicit statutory provisions that define who has the authority to impose an Internet shutdown, what justifications are legally acceptable and how oversight mechanisms can be implemented to prevent arbitrary shutdowns.

### iii. Limited public oversight and transparency

Building on the need to protect fundamental rights, it is essential to address the role of regulatory bodies in managing Internet shutdowns. To this end, the Communications Authority of Kenya (CA) must strengthen its regulatory oversight by clarifying its role during Internet shutdowns and ensuring robust regulatory procedures. Clear guidelines and procedures should be established to manage these situations effectively and fairly.

Simultaneously, telecommunication companies should take a proactive stance by resisting unwarranted government directives and refraining from sharing customer data in contravention of the Kenya Information and Communications Act 1998.[49]

Additionally, they should maintain transparency regarding government requests for data or directives to shut down services. This approach protects customer privacy and ensures companies act in the best interests of their users.

### iv. Negative socio-economic impact

Governments often mistakenly believe that Internet shutdowns will quell unrest, stop the spread of misinformation, reduce harm from cybersecurity threats, or curb cheating in the case of exam-related shutdowns in Algeria. But shutdowns are highly disruptive to economic activity. They halt e-commerce, generate losses in time-sensitive transactions, increase unemployment, interrupt business-customer communications, and create financial and reputational risks for companies.[50]

Similar to the situation in India, Internet shutdowns in Kenya have disrupted businesses, interfered with financial transactions, and undermined access to essential services. During the shutdown witnessed on 26th June, with disruptions evidenced with mobile money services, credit and debit card transactions, and e-commerce platforms were all inaccessible, the Internet Society estimates that such outages could cost Kenya approximately $6.3 million in lost GDP per day.[51]

---

48 Bailey, Rishab & Parsheera, Smriti. 'Data localisation in India: Questioning the means and ends,' (Working Papers 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18-242.html/> accessed 22 February 2025

49 Kenya Information and Communications Act 1998 (c 411A) s 31

50 Robert Mitchelle, 'The Real Impact of Internet Shutdowns'(*Internet Society*, 28 June 2023) <https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/> accessed 21 February, 2025

51 Mwenda Kivuva, 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations'(*KiC-TAnet*, 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinance-bill2024-demonstrations/> accessed 21 February 2025

### v. Transparency and Accountability

Several African countries, like Kenya, often justify Internet shutdowns on the grounds of national security and public order. In Kenya, national security is defined under Article 238 of the Constitution as "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability, prosperity, and other national interests."[52] The Constitution further provides that national security must conform to constitutional principles, follow the highest human rights standards, and respect the diversity of cultures.

Any Internet shutdown in Kenya justified under the pretext of national security must therefore meet constitutional standards, including the three-part test of legality, proportionality, and necessity when limiting human rights such as freedom of expression and access to information.[53]

For instance, Article 24(2) of the Constitution requires that any law limiting rights must be specific about the right being curtailed and the purpose of such limitation, ensuring that it does not undermine the core content of the affected right.

The case of *Okuta v Republic*[54] demonstrated the application of the proportionality test in evaluating whether pre-2010 laws remained justifiable under the new constitutional framework. The court found that the availability of alternative legal mechanisms, such as the National Cohesion and Integration Act and provisions on national security, could achieve the same objectives without resorting to outdated and potentially unconstitutional laws.

Despite these constitutional safeguards, Kenya's law enforcement agencies, including the National Security Council (chaired by the President), the Directorate of Criminal Investigations, and the National Intelligence Service, have faced criticism for their role in past Internet shutdowns.

This raises fundamental questions about the legal authority under which such orders were issued and whether they complied with constitutional and statutory requirements.

The Executive, through the Ministry of ICT, has established the ICT Authority as a state corporation under Legal Notice 183 of 2013, tasked with supervising the design, development, and implementation of critical ICT projects across the public sector. Additionally, the Communications Authority of Kenya (CA), established under the Kenya Information and Communications Act of 1998, serves as the statutory regulator of the ICT sector. It oversees the dissemination and management of information within the industry, including content shared on social media platforms.

Beyond government agencies, private corporations such as telecommunications companies and Internet service providers (ISPs) play a crucial role in enforcing shutdown orders. This raises significant concerns about the legality of such directives, whether due process was followed, and the extent of accountability among state and non-state actors. The involvement of private entities in executing shutdowns further complicates the issue of transparency, as decisions affecting public access to information are often made without sufficient public scrutiny or judicial oversight. Ultimately, transparency and accountability in Kenya's Internet governance framework become paramount.

## Communications Authority of Kenya(CAK)

Sections 23 and 25 of the KICA, mandate the CA to protect the interests of all users of telecommunications services in Kenya with respect to tariffs, quality of service and availability of diverse products and services among others. This oversight is mainly achieved through grant of licenses and monitoring and enforcement of the various license conditions.

---

52 Constitution of Kenya 2010.

53 ibid

54 *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR (Petition No. 397 of 2016)

The #RejectFinanceBill2024 protests in Kenya were a significant political event marked by widespread public opposition to new tax measures proposed in the Finance Bill 2024. During the anti-tax protests against the Finance Bill 2024, concerns arose about a potential Internet shutdown.[55] The Communications Authority of Kenya (CA), through its director general, assured the public that there were no intentions to disrupt Internet services, aligning any such action with an infringement of the Constitution.[56] Despite this, disruptions occurred[57], raising questions about the true intentions behind the actions.

The recent Internet shutdowns can be attributed to several factors, despite official statements denying intentional plans. Firstly, and more importantly, government intervention appears to be a significant cause, as the disruptions suggest deliberate action to control the flow of information.[58] This starkly contrasts with official denials, which claimed no such plans were in place.

The Communications Authority is established as an independent body that should ideally not maintain functional or financial interests with the executive or commercial interests. This objective is achieved through independent appointment of the Board and economic autonomy as the Regulator is funded by licence fees that it collects from licensees or directly from the national budget.[59] However, Section 5C of KICA grants the Cabinet Secretary an avenue to issue policy guidelines to the Authority.

Having witnessed actual Internet shutdown in Kenya, the regulator must maintain its independence in making decisions about the Internet. This can be achieved through transparency in decision making, that is, explaining explicitly the legal basis, nature and extent of controls to the Internet and communication technologies.

## Telecom Providers

Telecommunications companies empower people to exercise freedom of expression, but they can also enable politically motivated attempts to control online information flow. Kenya is a champion of the digital economy and has a strong reputation for putting technology to work for people's rights and interests. Telcos have a duty to reject government orders for a shutdown and respect human rights. They also have several tools to ensure this pushback is effective. Safaricom and Airtel are both parties to the United Nations Global Compact, which includes a commitment to respect and protect "internationally proclaimed human rights." Experts at the U.N. have explicitly affirmed that human rights apply online and have condemned Internet shutdowns.

A new report by U.N. special rapporteur David Kaye finds that shutdowns "involve measures to intentionally prevent or disrupt access to or dissemination of information online *in violation of human rights law*." Given these statements, we believe that telcos that are party to the Global Compact must refrain from intentionally disrupting networks.[60]

The role of communications companies in these protests is not only about Internet connectivity. Safaricom, Kenya's dominant telecommunications provider, has been blamed for sharing data with law enforcement facilities to facilitate the surveillance and abduction of people linked to the anti-finance bill movement. Safaricom has denied these claims, but the Office of the Data Protection Commissioner has yet to investigate

---

55 Kenyans.co.ke, 'Communications Authority of Kenya Assures Public There Will Be No Internet Shutdown,' <https://www.kenyans.co.ke/news/101971-govt-addresses-internet-shutdown-nairobi-during-finance-bill-protests> accessed 22 February 2025

56 ibid

57 Cloudflare Radar, 'Outage Center: Internet outages and traffic anomalies- 25th June 2024,' <https://radar.cloudflare.com/outage-center?dateStart=2024-06-25&dateEnd=2024-06-25> accessed 22 February 2025

58 Association for Progressive Communications, 'Digital protests, access and freedoms in Kenya,' <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 22 February 2025

59 Grace Mutung'u and others, 'Building trust between the state and citizens: A policy brief on Internet shutdowns and elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

60 Tinuola Dada and Peter Micek, 'Election watch: If Kenya orders an Internet shutdown, will telcos help #KeepItOn?' (*AccessNow*, 26 July 2017) <https://www.accessnow.org/election-watch-kenya-orders-internet-shutdown-will-telcos-help-keepiton/%3eaccessed> 22 February 2025

the complaints.[61] As of 27 June 2024, some abducted protesters linked to the movement are still missing, raising concerns about telecom accountability and transparency in executing government directives.

To improve transparency, telecom operators should consider informing subscribers in advance of potential service disruptions and involving them, where possible, in discussions with other stakeholders to avert shutdowns. In the event of a government-ordered shutdown, mobile network operators (MNOs) should disclose the nature and extent of the disruption and engage in dialogue with affected users about its impact. AccessNow, a digital rights advocacy group, has proposed a ten-point plan to guide telecom operators in upholding human rights.

This includes mechanisms for handling customer grievances, policies ensuring timely investigations, and provisions for compensating those affected by service disruptions. While companies like Safaricom do compensate subscribers for general service outages, it remains unclear whether compensation applies in cases of government-mandated shutdowns. This question could be addressed through a consultative process involving all affected stakeholders.

Ultimately, resolving these challenges requires further study of dispute resolution mechanisms for regulatory actions and checks and balances on the regulator as an independent constitutional body. Additionally, greater transparency in the licensing process is needed to ensure that telecom operators are not compelled to take actions that could potentially violate human rights.[62]

## Case Studies on Internet Shutdowns and Their Implications for Kenya

### 1. Kenya's 2017 General Election and Internet Disruptions

Concerns over digital restrictions and potential interference with online communications marked Kenya's 2017 general elections. Reports from digital rights organisations such as Access Now and Article 19 indicate that government agencies allegedly pressured telecom providers to restrict access to social media and messaging platforms, particularly during heightened political activity.

This phenomenon aligns with broader global trends where states resort to Internet shutdowns to control information flows, particularly during elections or civil unrest. The documented patterns of state-driven digital repression situate Kenya's case within a larger framework of governments leveraging Internet disruptions to influence political discourse and suppress dissent.[63] Furthermore, the use of Internet disruptions raises concerns about the violation of fundamental rights, including freedom of expression and access to information, as protected under Articles 33 and 35 of the Kenyan Constitution and international human rights instruments such as the African Charter on Human and Peoples' Rights (ACHPR).

### 2. Uganda's 2021 Election and Its Implications for Kenya

Although not a Kenyan case, Uganda's 2021 general elections offer critical insights into regional Internet governance challenges. The Ugandan government imposed a total Internet shutdown on January 13, 2021, just before the election, effectively cutting off communication for several days. Human Rights Watch (2021) and other advocacy groups condemned the move, noting its impact on transparency, election monitoring, and the free flow of information.[64]

---

61 Mwenda Kivuva, 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations'(*KiCTAnet,* 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinance-bill2024-demonstrations/> accessed 21 February 2025

62 Grace Mutung'u and others, 'Building trust between the state and citizens: A policy brief on Internet shutdowns and elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

63 Freedom House, 'Key Developments, June 1, 2017 - May 31, 2018', <https://freedomhouse.org/country/kenya/freedom-net/2018> accessed 22 February 2025

64 World Report 2022: Uganda (Human rights Watch) <https://www.hrw.org/world-report/2022/country-chapters/uganda> accessed 22 February 2025

The Ugandan shutdown raised serious concerns for Kenya due to shared telecommunications infrastructure and business interests. Kenyan telecom providers such as Safaricom and Airtel, which operate in Uganda, faced scrutiny over their role in enforcing the blackout. This case underscores the potential for similar actions in Kenya, especially given precedents in restricting online spaces during politically sensitive periods. Additionally, it highlights the broader East African regulatory landscape, where governments may draw inspiration from each other's digital governance approaches.

### 3. India's Internet Shutdowns

India, widely regarded as the global leader in Internet shutdowns, presents a legal framework that could influence Kenya's judicial and regulatory approach. The landmark case of ***Anuradha Bhasin v. Union of India (2020)***[65] set an important precedent. The court ruled that indefinite Internet shutdowns violate constitutional freedoms and must adhere to the principles of necessity and proportionality.

The judgment emphasised that any restriction on Internet access must be (a) based on clear legal grounds, (b) subject to judicial review, and (c) implemented as a last resort.

Given Kenya's Constitutional Article 24 on limitations of rights,[66] this ruling could serve as a reference for future legal challenges against government-imposed Internet disruptions in Kenya. It also aligns with the Kenyan High Court's 2021 decision in ***Bloggers Association of Kenya v. Attorney General***[67] where the court ruled to protect digital rights against state overreach.

## Human Rights Impact.

From time to time, governments across the world's respect for human rights has been tested in several ways. Still, arguably, nothing has tested it more than the rise of civil activities that take place over the Internet.[68] As highlighted earlier, the Internet has become indispensable for communication, education, business, and even political participation. It has enabled individuals to freely and more easily do almost everything with a click of a button or a tap on a screen.

Expectedly, these powers and opportunities that the Internet has given to individuals are prone to abuse, and to prevent such abuse, laws have allowed governments to use disruptive measures such as Internet shutdowns.[69]

On the flipside, though, these measures are applied haphazardly without clear regulations and cause gross human rights violations as discussed hereunder.

Various justifications are given by governments whenever they intentionally disrupt the Internet (partial or total blackouts), including national security concerns, prevention of misinformation and curbing civil unrest, among others.[70] The broader adverse consequences of this are twofold: Firstly, the indeterminate nature of these justifications acts as a loophole for abuse of power; and secondly, these actions disproportionately affect socio-economic rights and fundamental freedoms, particularly among vulnerable populations. For example, in the age of e-commerce, small businesses such as those that rely on social media and digital platforms for marketing and transactions suffer significant losses during these shutdowns.[71]

---

65 Anuradha Bhasin v Union of India AIR 2020 SC 1308

66 Constitution of Kenya, 2010.

67 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR (Kenya)

68 Ewan Sutherland, 'The Internet and Human Rights: Access, Shutdowns, and Surveillance' (WG Hart Legal Workshop 2018, London, 11-12 June 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203883> accessed 22 February 2025

69 ibid

70 Office of the United Nations High Commissioner for Human Rights (OHCHR), 'Dramatic Real-Life Effects of Internet Shutdowns on People's Lives and Human Rights' (Press Release, 23 June 2022) <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human > accessed 22 February 2025

71 Ibid

Furthermore, rural women and children who depend on digital resources for education, healthcare, and economic empowerment get lockedout whenever Internet shutdowns occur.[72]

As the population using the Internet continues to grow, there is a need to protect their fundamental rights. Indeed, this has been recognised under international law with institutions such as the United Nations Human Rights Council (UNHRC) affirming that "the same rights that people have offline must also be protected online, in particular freedom of expression."[73] The **International Covenant on Civil and Political Rights (ICCPR, 1966)** further provides that:

"*Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*"[74]

This right is to be exercised without unwarranted interference unless it is for the sake of respect of the rights or reputations of others; protection of national security or public order (ordre public), or of public health or morals.[75] While these interferences are supposed to set limits when a right is exercised at the expense of the rights of others, Internet shutdowns end up being used as tools of control, which undermine human rights more than they protect them.[76] As such, they should be cautiously utilised and, in most cases, they should only be used as a last resort.

Furthermore, the effects of Internet outages go beyond the short-term interruptions. They worsen the digital divide by restricting opportunities for economic involvement and disproportionately harming members of vulnerable communities. For instance, when the Internet connection is cut off during elections, demonstrations, or emergencies, it hinders transparency and reduces civic participation, preventing people from making reasoned decisions. Such outrageous acts must be seen as a violation of Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the Universal Declaration of Human Rights (UDHR, 1948), among other laws.

Although this right is recognised under the umbrella of access to information and freedom of expression, it is also related to other rights, such as socio-economic rights. The focus lies on freedom of expression and access to information while demonstrating how any interference with these rights has a ripple effect towards other rights.

## Rights under International Law

Since the Constitution of Kenya has accepted international laws to form part of Kenyan laws, accessing the Internet as a right is protected under various international instruments, as already observed.[77] This is guaranteed through fundamental rights and freedoms like free speech and access to information. To contextualise this, the UDHR, for example, under Article 19, guarantees the right to freedom of expression.[78] The same is reinforced under Article 19 (2) of the ICCPR, which reinforces this principle in Article 19(2), which protects the right to seek, receive, and impart information and ideas of all kinds, regardless of frontiers.[79]

---

72 Advocacy Assembly, 'The gendered impact of Internet shutdowns' (Advocacy Assembly, 2023) <https://advocacyassembly.org/en/news/245> accessed 23 February 2025

73 United Nations Human Rights Council (UNHRC), 'The promotion, protection and enjoyment of human rights on the Internet' (27 June 2016) UN Doc A/HRC/RES/32/13

74 International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, 999 UNTS 171, art 19(2)

75 Ibid

76 Jay T. Conrad, 'A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)' (2023) 13 *Seattle Journal of Technology, Environmental & Innovation Law* 2

77 Constitution of Kenya 2010, Art 2 (6).

78 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) Art 19.

79 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19(2)

Moreover, the General Comment No. 34 (2011) by the Human Rights Committee has interpreted this provision explicitly by stating:[80]

"Paragraph 2 protects all forms of expression and the means of their dissemination. Such forms include spoken, written, and sign language, as well as non-verbal expressions such as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. They include all forms of audio-visual as well as electronic and Internet-based modes of expression."[81]

Furthermore, it encourages States parties to take account that the extent to which developments in information and communication technologies, such as Internet and mobile-based electronic information dissemination systems, have substantially changed communication practices around the world.[82] Therefore, states should be cautious against arbitrary Internet restrictions limiting this freedom. Any limitations on Internet access must be necessary, proportionate, and in line with international human rights standards.

Continentally, the African Charter on Human and Peoples' Rights provides for the right to access information under Article 9.[83] It states that every individual has a right to receive information and freely express their opinions. Furthermore, the African Declaration on Internet Rights and Freedoms (2014) advocates for the promotion of Internet accessibility, digital inclusion, and the protection of online freedoms.[84] This declaration urges African states to refrain from arbitrary shutdowns and states that everyone should enjoy unrestricted access to the Internet.[85] Any shutting down or blocking of access to social networking platforms, and in fact, the Internet in general, constitutes a direct interference with this right. Free and open access to the Internet must therefore always be protected.

The African Commission on Human and Peoples' Rights has also reiterated the significance of the rights and freedoms guaranteed under Article 9 of the African Charter, which are to be enjoyed even in the digital space.[86] States must protect them, and state-imposed restrictions must meet the standards of legality, necessity, and proportionality. In the Commission's Resolution 362 (2016) on the Right to Freedom of Information and Expression on the Internet in Africa, there is explicit condemnation of the disruption of the Internet as a tool to suppress dissent and hinder access to information and freedom of expression.[87]

The same has a ripple effect that even affects other rights. For instance, children under the Competency-Based Curriculum may run into problems in their studies as they heavily rely on materials available online.[88] On top of that, many Micro, Small and Medium Enterprises (MSMEs) which constitute 98% of all business, create 30% of jobs annually and contribute 40% towards the country's GDP are have in the recent past heavily relied on the Internet for marketing and transactions and any shutdown of the Internet jeopardise their potential and their contribution to the economy[89]. Rightly then, the Commission emphasises the need for states to be hesitant when it comes to Internet shutdowns.

---

80 UN Human Rights Committee, 'General Comment No. 34: Article 19, Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34, para 12.

81 ibid

82 Ibid

83 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5, Art 9.

84 African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (adopted 10 November 2019)

85 Ibid

86 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5, Art 9

87 African Commission on Human and Peoples' Rights, 'Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa' (4 November 2016) ACHPR/Res.362(LIX)2016

88 Kenya Institute of Curriculum Development, 'Competency-Based Curriculum Materials' <https://kicd.ac.ke/cbc-materials/> accessed 23 February 2025

89 Kenya National Bureau of Statistics, '2016 Micro, Small and Medium Enterprises (MSME) Survey Basic Report' (2016) <https://www.knbs.or.ke/2016-micro-small-and-medium-enterprises-msme-survey-basic-report/ > accessed 23 February 2025.

## Rights under the Constitution and Kenyan Laws

Key and essential provisions of the Constitution of Kenya that can be interpreted to guarantee access to the Internet are under Article 33 and 35 on freedom of expression and right to access information, respectively. Article 33 provides that every person has the right to freedom of expression, which includes: freedom to seek, receive or impart information or ideas;[90] freedom of artistic creativity;[91] and academic freedom and freedom of scientific research.[92] This right however does not extend to: propaganda for war;[93] incitement to violence;[94] hate speech;[95] or advocacy of hatred that either constitutes ethnic incitement, vilification of others or incitement to cause harm; or is based on any ground of discrimination specified or contemplated in Article 27(4).[96]

Article 35 then guarantees the right of access to: information held by the State;[97] and information held by another person and required for the exercise or protection of any right or fundamental freedom.[98]

It is already established in law that a right or a fundamental freedom cannot be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. [99] The unjustified nature of limitations of these rights, as observed in this paper, is a gross violation of the Constitution and the rule of law and causes a disruption even in enjoying other rights and freedoms.

To demonstrate this disruption, the right to property, as enshrined in Article 40 of the Constitution, is one of the social and economic rights compromised by Internet shutdowns.[100] Where businesses that rely on the Internet are undermined. Other rights under this category, such as access to education, healthcare, and economic participation, are also affected negatively by Internet shutdown.[101] Finally, Article 46, which deals with consumer rights, requires that citizens get access to quality goods and services, which is violated in cases such as where mobile banking, e-commerce, and other digital services are disrupted due to an Internet shutdown.[102]

Digital rights are fundamental human rights, and as such, not absolute. As with most rights, they may be lawfully restricted where the restrictions are reasonable and justifiable in an open and democratic society.

Article 24 of the Constitution stipulates that limitations should align with the principles of legality, necessity and proportionality. Further, as confirmed in General Comment 34 and Principle 9 of the African Declaration,[103] the restrictions that states impose should not jeopardise these rights. In practice, this requires that any measures limiting digital rights, such as Internet shutdowns, surveillance, or content blocking, must be transparent, subject to judicial oversight, and accompanied by precise mechanisms for accountability and redress.

---

90 Constitution of Kenya 2010, Art 33 (1) (a).

91 Ibid, Art 33 (1) (b).

92 Ibid, Art 33 (1) (c).

93 Ibid, Art 33 (2) (a).

94 Ibid, Art 33 (2) (b).

95 Ibid, Art 33 (2) (c).

96 Ibid, Art 33 (2) (d).

97 Ibid, Art 35 (1) (a).

98 Ibid, Art 33 (1) (b).

99 Ibid, Art 24 (1); *In the Matter of the Principle of Gender Representation in the National Assembly and the Senate* [2012] KESC 5 (KLR).

100 Constitution of Kenya 2010, Art 40.

101 Ibid, Art 43.

102 Ibid, Art 46.

103 African Declaration no.6.

Although there is an expansive legal framework, enforcement of the same remains a challenge. The randomness at which the government shuts down the Internet has excellent implications, including the erosion of investor confidence, deterrence of innovation, and stifling economic growth.

# REFERENCES


**Books**

1. Balkin JM, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society* (Routledge 2017)

**Journal Articles**

2. Bhatia KV and others, 'Protests, Internet Shutdowns, and Disinformation in a Transitioning State' (2023) 45 *Media, Culture & Society* 1101
3. Conrad JT, 'A New Right is the Wrong Tactic: Bring Legal Actions Against States for Internet Shutdowns Instead of Working Towards a Human Right to the Internet (Part 1)' (2023) 13 *Seattle Journal of Technology, Environmental & Innovation Law* 2
4. Gwagwa A and others, 'Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions' (2020) 26 *African Journal of Information and Communication* 3
5. Hardwaj S and others, 'Rising Internet Shutdowns in India: A Legal Analysis' (2020) 16 *Indian Journal of Law and Technology* 1
6. Sugow A and others, 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression' (2021) 1 *Journal of Intellectual Property and Information Technology Law* 1

**Cases**

7. *Anuradha Bhasin v Union of India* AIR 2020 SC 1308
8. *Association des Blogueurs de Guinee (ABLOGUI) v State of Guinea* [2023] ECOWASCJ 1
9. *Bloggers Association of Kenya (BAKE) v Attorney General* [2020] eKLR
10. *Geoffrey Andare v Attorney General* [2016] eKLR
11. *In the Matter of the Principle of Gender Representation in the National Assembly and the Senate* [2012] KESC 5 (KLR)
12. *Jacqueline Okuta v Attorney General* [2017] eKLR

**Legislation**

13. Computer Misuse and Cybercrimes Act 2018 (Kenya)
14. Constitution of Kenya 2010
15. Data Protection Act 2019 (Kenya)
16. Kenya Information and Communications Act 1998 (Kenya)
17. National Cohesion and Integration Act 2008 (Kenya)
18. Prevention of Terrorism Act 2012 (Kenya)

**International Treaties and Conventions**

19. African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) OAU Doc CAB/LEG/67/3 rev 5

20. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

21. Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)

**Official Documents**

22. African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (10 November 2019)

23. African Commission on Human and Peoples' Rights, 'Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa' (4 November 2016) ACHPR/Res.362(LIX)2016

24. Ruggie J, 'Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises' (21 March 2011) UN Doc A/HRC/17/31

25. UNGA Res 78/213 (22 December 2023) UN Doc A/RES/78/213

26. UNHRC, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UN Doc A/HRC/RES/32/13

27. UN Human Rights Committee, 'General Comment No. 34: Article 19, Freedoms of Opinion and Expression' (12 September 2011) UN Doc CCPR/C/GC/34

**Reports**

28. ARTICLE 19, 'Getting Connected: Freedom of Expression, Telcos and ISPs' (June 2017) <https://www.article19.org/wp-content/uploads/2017/06/Getting-Connected-2.pdf> accessed 7 April 2025

29. ARTICLE 19, 'Kenya: Release and Cease Attacks on Edwin Mutemi wa Kiama' (8 April 2021) <https://www.article19.org/resources/kenya-cease-attacks-on-and-release-edwin-mutemi-wa-kiama/> accessed 18 March 2025

30. Freedom House, 'Kenya: Freedom on the Net 2024 Country Report' (Freedom House 2024) <https://freedomhouse.org/country/kenya/freedom-net/2024> accessed 22 February 2025

31. Human Rights Watch, 'Kenya: Police Threaten Activists Reporting Abuse' (4 June 2018) <https://www.hrw.org/news/2018/06/04/kenya-police-threaten-activists-reporting-abuse> accessed 22 February 2025

32. Human Rights Watch, 'No Internet Means No Work, No Pay, No Food' (14 June 2023) <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic> accessed 20 February 2025

33. Kenya National Bureau of Statistics, '2016 Micro, Small and Medium Enterprises (MSME) Survey Basic Report' (2016) <https://www.knbs.or.ke/2016-micro-small-and-medium-enterprises-msme-survey-basic-report/> accessed 23 February 2025

34. Mutung'u G and others, 'Building Trust between the State and Citizens: A Policy Brief on Internet Shutdowns and Elections in Kenya 2017' (KiCTAnet 2017) <https://www.kictanet.or.ke/wp-content/uploads/2017/09/Kenya_Policy_Brief_On_Internet_Shutdowns.pdf> accessed 22 February 2025

**Conference Papers**

35. Sutherland E, 'The Internet and Human Rights: Access, Shutdowns, and Surveillance' (WG Hart Legal Workshop, London, 11-12 June 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203883> accessed 22 February 2025

**Websites**


36. '6 Media Houses Warned over Coverage of Azimio Mass Action Protest' (Pulselive Kenya, 29 July 2024) <https://www.pulselive.co.ke/articles/news/local/citizen-tv-ntv-k24-kbc-tv47-and-ebru-tv-warned-over-coverage-of-azimio-protest-2024072908514395101> accessed 15 February 2025

37. 'Communications Authority of Kenya Assures Public There Will Be No Internet Shutdown' (Kenyans.co.ke) <https://www.kenyans.co.ke/news/101971-govt-addresses-internet-shutdown-nairobi-during-finance-bill-protests> accessed 22 February 2025

38. 'Competency-Based Curriculum Materials' (Kenya Institute of Curriculum Development) <https://kicd.ac.ke/cbc-materials/> accessed 23 February 2025

39. 'Digital Protests, Access and Freedoms in Kenya' (Association for Progressive Communications) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 22 February 2025

40. 'Digital Protests, Access and Freedoms in Kenya' (APC, 18 July 2024) <https://www.apc.org/en/news/digital-protests-access-and-freedoms-kenya> accessed 18 March 2025

41. 'Dramatic Real-Life Effects of Internet Shutdowns on People's Lives and Human Rights' (OHCHR, 23 June 2022) <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human> accessed 22 February 2025

42. 'Election Watch: If Kenya Orders an Internet Shutdown, Will Telcos Help #KeepItOn?' (AccessNow, 26 July 2017) <https://www.accessnow.org/election-watch-kenya-orders-internet-shutdown-will-telcos-help-keepiton/> accessed 22 February 2025

43. 'Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?' (Carnegie Endowment for International Peace, March 2022) <https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en> accessed 18 March 2025

44. 'Internet Shutdowns in Africa: Addressing the Human Rights Responsibilities of Telecoms Companies' (Business and Human Rights Resource Centre, 10 May 2023) <https://www.business-humanrights.org/en/from-us/briefings/internet-shutdowns-in-africa-addressing-the-human-rights-responsibilities-of-telecoms-companies/> accessed 20 February 2025

45. 'Kenya Borrows Leaf From Peers on Internet Restriction' (The East African, 27 June 2024) <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-borrows-leaf-from-peers-on-internet-restriction-4671858> accessed 22 February 2025

46. 'Kenya Plans to Place Public Security above Data Privacy. That's a Bad Idea' (The Conversation, 11 February 2019) <http://theconversation.com/kenya-plans-to-place-public-security-above-data-privacy-thats-a-bad-idea-111099> accessed 17 February 2025

47. 'Key Developments, June 1, 2017 – May 31, 2018' (Freedom House) <https://freedomhouse.org/country/kenya/freedom-net/2018> accessed 22 February 2025

48. 'Manhandled and Choked – Tanzanian Activist Recounts Abduction' (BBC News, 13 January 2025) <https://www.bbc.com/news/articles/cd7dxz48e01o/> accessed 20 February 2025

49. 'Outage Center: Internet Outages and Traffic Anomalies – 25th June 2024' (Cloudflare Radar) <https://radar.cloudflare.com/outage-center?dateStart=2024-06-25&dateEnd=2024-06-25> accessed 22 February 2025

50. 'Proposal to Block Websites and Applications Threatens Kenya's Digital Ecosystem' (KiCTAnet, 2 October 2024) <https://www.kictanet.or.ke/proposal-to-block-websites-and-applications-threatens-kenyas-digital-ecosystem/> accessed 23 February 2025

51. 'Proposed Changes to Kenya's Constitution: A Look at the 2024 Amendment Bill' (Sharp Daily, 2 October 2024) <https://thesharpdaily.com/kenya-constitutional-amendment-bill-2024/> accessed 23 February 2025

52. 'State Surveillance: Kenyans Have a Right to Privacy – Does the Government Respect It?' (The Conversation, 29 November 2024) <https://www.polity.org.za/article/state-surveillance-kenyans-

have-a-right-to-privacy-does-the-government-respect-it-2024-11-29> accessed 17 February 2025

53. 'Surge in Abductions of Government Critics in Kenya Sparks Mass Public Outcry' (Peoples Dispatch, 14 January 2025) <https://peoplesdispatch.org/2025/01/14/surge-in-abductions-of-government-critics-in-kenya-sparks-mass-public-outcry/> accessed 17 February 2025

54. 'Technology-Facilitated Rights and Digital Authoritarianism: Examining the Recent Internet Shutdown in Kenya' (CIPIT, 9 August 2024) <https://cipit.org/technology-facilitated-rights-and-digital-authoritarianism-examining-the-recent-internet-shutdown-in-kenya/> accessed 15 February 2025

55. 'The Gendered Impact of Internet Shutdowns' (Advocacy Assembly, 2023) <https://advocacyassembly.org/en/news/245> accessed 23 February 2025

56. 'The Real Impact of Internet Shutdowns' (Internet Society, 28 June 2023) <https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/> accessed 21 February 2025

57. 'Uganda Election: Facebook and WhatsApp Blocked' (BBC News, 18 February 2016) <http://www.bbc.com/news/world-africa-35601220> accessed 18 March 2025

58. 'Uganda: Opposition Politician Charged after Abduction: Kizza Besigye' (Amnesty International, 26 November 2024) <https://www.amnesty.org/en/documents/afr59/8779/2024/en/> accessed 17 February 2025

59. 'Urgent Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 Demonstrations' (KiCTAnet, 26 June 2024) <https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinancebill2024-demonstrations/> accessed 21 February 2025

60. 'Why Has Kenya's Finance Bill Triggered Protests?' (Context.news, 26 June 2024) <https://www.context.news/money-power-people/why-has-kenyas-finance-bill-triggered-public-outrage> accessed 17 February 2025

61. Bailey R and Parsheera S, 'Data Localisation in India: Questioning the Means and Ends' (Working Paper 18/242, National Institute of Public Finance and Policy 2018) <https://ideas.repec.org/p/npf/wpaper/18/242.html> accessed 22 February 2025

62. Council of Europe, 'The Role of Internet Intermediaries as Gatekeepers to Freedom of Expression – Conference in Vienna' (2017) <https://www.coe.int/en/web/freedom-expression/home/-/asset_publisher/RAupmF2S6voG/content/the-role-of-internet-intermediaries-as-gatekeepers-to-freedom-of-expression-conference-in-vienna> accessed 17 February 2025

63. Directorate of Criminal Investigations, 'Statement on Arrest of Edgar Obare under Section 23 of Computer Misuse and Cybercrimes Act 2018' (X, 4 March 2021) <https://twitter.com/dci_kenya/status/1367512899044925442> accessed 18 March 2025

64. World Report 2022: Uganda (Human Rights Watch) <https://www.hrw.org/world-report/2022/country-chapters/uganda> accessed 22 February 2025


The Kenyan Section of the International Commission of Jurists (ICJ Kenya)
ICJ Kenya House, Off Silanga Road, Karen
P.O. Box 59743 - 00200, Nairobi, Kenya
www.icj-kenya.org

ICJ Kenya