Digital Democracy Initiative

Strengthening Support Ecosystems for Digital Democracy in Côte d'Ivoire

A Case Study Assessment Report

March 2025

CIVICUS

Acknowledgments

RESEARCH TEAM

Verengai Mabika, Augustus Emenogu, Steven Akomain, Rahma Moussa

DESIGN AND LAYOUT

Sol Mokdad

We would like to acknowledge and thank all the representatives from civil society organisations and Human Rights Defenders who participated in the surveys and interviews for this research.

Digital Democracy Initiative

The Digital Democracy Initiative (DDI) is a programme to safeguard inclusive democracy and human rights in the digital age. It focuses on supporting local civil society in the Global South, particularly in countries undergoing democratic regression and where civic space is under pressure. For more information visit digitaldemocracyinitiative.net

CIVICUS

CIVICUS is a global alliance of civil society organisations and activists working to strengthen citizen action and civil society throughout the world. For more information visit civicus.org

Expectation State

Expectation State takes a different approach to inclusive growth in emerging states, benefiting society. We are an employee-owned business of committed development experts rooted in our countries. For more information visit expectationstate.com

Acronyms

ADC-CI	Aide, Assistance et Développement Communautaire de Côte d'Ivoire
AFJ-CI	Amnesty International-Côte d'Ivoire
APDH	Association des Femme Juristes de Côte d'Ivoire
APDL	Action pour la Protection des Droits de L'Homme
BTI	Bertelsmann Transformation Index
CNDH	Convention Nationale des Droits de l'Homme
CSOs	Civil Society Organisations
CSCI	Convention de la Société Civile de Côte d'Ivoire
DPI	Deep Packet Inspection
ES	Expectation State
EU	European Union
HRD	Human Rights Defender
KAS	Konrad Adenauer Stiftung
MIDH	Mouvement Ivoirien des Droits Humains Côte d'Ivoire
NGOs	Non-Governmental Organisations
OSIWA	Open Society Initiative for West Africa
RIDDEF	Réseau Ivoirien des Droits de l'Enfant et de la Femme
VPNs	Virtual Private Networks
WACSI	West Africa Civil Society Institute
WAIGF	West Africa Internet Governance Forum

Contents

1.0 Introduction

1.1 Background

Digital technologies have fundamentally transformed the landscape of democracy, (Lungu, P.C., 2024). The Internet and associated tools are potent platforms that foster civic engagement, promote transparency, and advocate for human rights. Civil society organisations (CSOs) have emerged as key players in this digital democracy movement, utilising technology to empower citizens, holding governments accountable, and building stronger civic communities, (Poisson M, 2024).

However, not everyone experiences the promise of digital democracy equally. In countries with limited democratic space, where governments restrict civil liberties and political participation, CSOs working on digital democracy encounter significant challenges. The could be described broadly three categories:

- **Legal and Regulatory Obstacles:** Governments often implement restrictive laws and regulations that hinder CSOs' ability to operate freely in the digital space. Governments in countries with limited democratic space may enact laws and regulations targeting digital activism. These laws can criminalise online dissent, restrict access to encrypted communication platforms, and impose heavy burdens on CSOs utilising technology for advocacy work. The threat of legal action can create a climate of fear and self-censorship, hindering the effectiveness of digital democracy efforts.

- **Technical and Infrastructure Barriers:** Limited internet access, poor digital infrastructure, and lack of technical expertise can impede CSOs' effective leveraging of digital tools.

- **Security and Privacy Concerns:** CSOs and their members may face surveillance, cyber-attacks, and other digital threats that compromise the safety and security of their data.

These challenges impact CSOs' work promoting digital democracy, particularly in countries with authoritarian tendencies or limited democratic freedoms. Despite these obstacles, many organisations continue to innovate and adapt, finding creative ways to use technology to advance their mission and protect civic spaces in the digital realm.

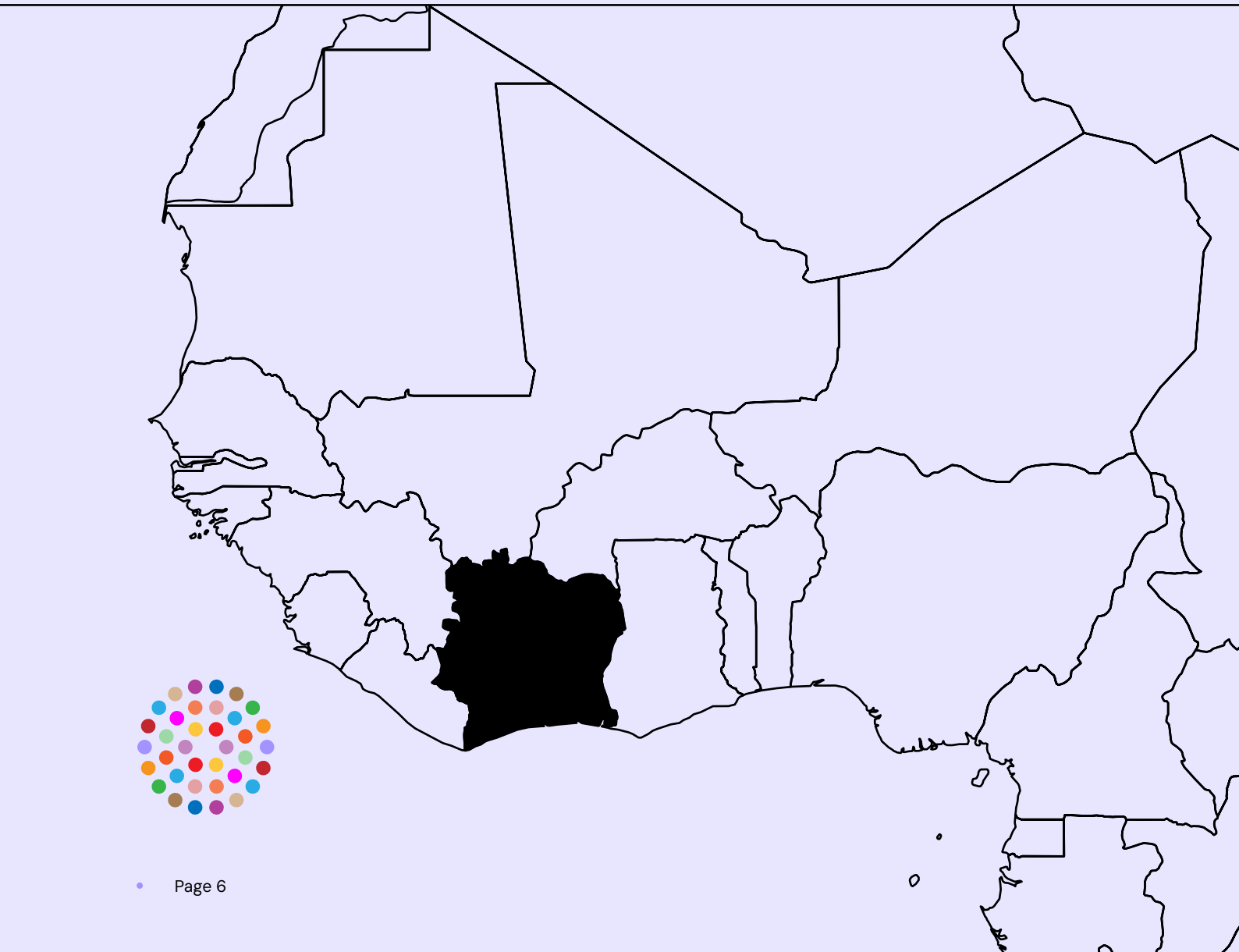
- **Restricted Operational Environment:** The CIVICUS Monitor framework categorizes civic space along a continuum of obstructed, repressed, and closed societies within which fundamental freedoms of expression, association, and assembly are frequently curtailed. This restrictive operational environment can significantly impede CSOs in their ability to function autonomously, secure legal registration, and mobilize financial resources. Furthermore, governmental limitations on internet access and the implementation of censorship measures can undermine CSOs' capacity to leverage digital technologies for their activities

- **Limited Resources and Capacity:** Despite limited resources, CSOs working on digital democracy in Côte d'Ivoire demonstrate remarkable resilience. These organisations face scarce funding for digital rights and advocacy work and struggle with restricted access to essential technologies and technical expertise by state actors. Nevertheless, they effectively utilise digital tools for secure communication, data analysis, and online campaigning. Their determination and resourcefulness inspire others as they overcome these challenges.

Côte d'Ivoire experienced a rating upgrade from the repressed to the obstructed category due to fewer reported civic space violations in recent years, (Civicus Monitor, n.d). In 2020, the country had a highly contested and controversial electoral period, which led to the country's downgrade to the repressed rating in December 2020. While there were incidents of protesters arrested in 2024, the country remains under the obstructed category, (Civicus Monitor, 2024). These episodes of arrests coupled with new regulations for CSOs operations in 2024 is increasingly creating a challenging environment for CSOs, journalists, and activists to freely express. To this end, CSOs in Côte d'Ivoire employ creative strategies to maximise their impact. They:

- Leverage open-source software and free online platforms to reduce costs
- Collaborate with international partners to access technical expertise
- Conduct grassroots fundraising campaigns to supplement limited funding
- Resort to online petitions and advocacy

CSOs are also prioritising digital security, implementing robust measures to protect their data and communications from potential surveillance or cyber-attacks.



1.2 Overview of Case Study Assessment

Digital technologies are reshaping the global democratic landscape. The internet and social media have become indispensable tools for civic engagement, empowering citizens to access information, voice their opinions, and organise political action. However, the influence of these technologies on democracy is complex and varies across contexts. In countries where democratic freedoms are restricted and civic participation is limited, the digital democracy landscape is particularly challenging, offering opportunities and obstacles for pro-democracy movements and civil society organisations.

This country's case study documents the support systems available to CSOs in Côte d'Ivoire. The study focuses on how these organisations champion digital democracy in an environment where authorities significantly curtail civic freedoms. It examines the current state of digital democracy in Côte d'Ivoire, highlighting the challenges CSOs face and their strategies to navigate this restrictive landscape. Insights from the country report are used to formulate actionable recommendations for enhancing global support of digital democracy.

The case study assessment involved a comprehensive literature review, data collection through key informant interviews, online surveys, and document analysis.

1.3 Case Study Methodology

1.3.1 Technical Approach

The Case Study Assessment applied aspects of co-design approaches, systems thinking, and human-centred design practice. The methodological approach ensured a thorough, rigorous, and context-sensitive assessment of the challenges and opportunities facing CSOs working on digital democracy in constrained environments. The technical approach combined data collection methods, robust analysis, and stakeholder engagement to produce actionable insights and recommendations for strengthening digital democracy efforts in Côte d'Ivoire.

1.3.2 Country Selection and Literature Review

The objective of the country selection process was to inform the identification of three (3) countries classified as 'Obstructed,' 'Repressed' or 'Closed' according to the CIVICUS Monitor data, a widely recognised source of information on civic space and civil society. The county selection focused on countries within the same region (sub saharan Africa) ensuring a broader yet region-specific perspective. Côte d'Ivoire faces restrictions on online freedoms and civic space. While there is some space for non-state media and editorial independence, journalists face the risk of physical attack and criminal defamation charges, which encourage self-censorship, (Civicus Monitor, n.d.). The archetypal digital democracy environments in Côte d'Ivoire are thus classified as being **Obstructed.**

This categorisation offers insights into the challenges and opportunities for promoting digital democracy in restrictive contexts. Beyond the identification of a suitable case country, a multi-tier approach was adopted involving a thorough review of data, close collaboration with CIVICUS, and consideration of various criteria to commence the case study assessment process:

- **Data Review:** Analysed CIVICUS Monitor data and other relevant global indices to shortlist potential countries.
- **Consultation with CIVICUS:** Collaborated closely with CIVICUS to ensure alignment with

strategic priorities and regional focus.

- **Criteria Consideration:** digital repression, active CSOs, the political landscape, and data availability.

1.3.3 Desk Review Process

An in-depth literature review was conducted to understand the current digital democracy, digital repression, and the support ecosystems for CSOs in the selected countries. The review followed these steps:

- **Document Collection:** gathered and reviewed existing literature, including academic papers, reports from international organisations, policy documents, and country-specific case studies.
- **Thematic Analysis:** The findings were categorised into central themes, such as operational challenges, resource limitations, legal frameworks, and successful strategies.
- **Contextual Understanding:** identified specific political and socio-economic factors influencing Côte d'Ivoire's digital landscape. The annexes include a list of reviewed documents.

1.3.4 Key Informant Interviews and Online Survey

Nine (9) key informant interviews were conducted with strategic stakeholders in Côte d'Ivoire. The low response rate encountered in securing interviews and online survey responses highlight the prevailing concerns among human rights activists and journalists regarding their safety in telling their stories. The research team could only engage with these actors by navigating trusted networks and respondent referrals.

1.3.5 Data Analysis and Reporting

The data analysis identified key themes, challenges, and opportunities for strengthening support ecosystems for digital democracy in the selected countries. This mixed methods approach involved both mainly qualitative analysis methods in addition to employing the triangulation verification of multiple data sources highlighted below:

- **Qualitative Analysis:** thematic analysis to identify common patterns and insights from interviews and document reviews. Employed Perplexity AI to organise and analyse qualitative data, ensuring a rigorous and systematic analysis process.
- **Quantitative Analysis:** analysed collated online survey data using statistical tools like SPSS to identify trends and correlations in CSO engagement, challenges, and support needs.
- **Triangulation:** Cross-verified data from multiple sources (interviews, online surveys, document reviews) to ensure validity and reliability of findings.

The case study assessment report identified existing support mechanisms for CSOs working on digital democracy, highlighting successful strategies and initiatives employed by CSOs to overcome digital repression and strengthen the support ecosystem. The report also offers context-specific recommendations for improving the support ecosystem for digital democracy in the chosen country.

2.0 Digital Democracy Ecosystem in Côte d'Ivoire

Côte d'Ivoire is experiencing a robust economic recovery after nearly a decade of conflict, yet the country continues to grapple with significant political and post-conflict challenges. Key priorities for the government include fostering political consensus, advancing national reconciliation, and ensuring long-term security, (BTI 2024). The 2020 electoral period was marred by a sharp escalation in violence, including civic space violations, representing a notable setback. However, in the subsequent years, there has been measurable progress in safeguarding civil liberties, with civil society organisations and political opposition groups operating with greater freedom following the conclusion of the elections.

By 2022, while President Alassane Ouattara had secured a third term, a move that sparked significant contestation and accusations of undermining democratic norms (International Crisis Group, 2020), the claim of consolidated leadership overlooks the deep seated political divisions persisting in Côte d'Ivoire. These divisions were starkly highlighted by the violent aftermath of the 2020 presidential elections, which saw numerous casualties and widespread protests against Ouattara's candidacy (Amnesty International, 2020).

The return of former President Laurent Gbagbo, acquitted by the International Criminal Court but still a powerful figure with considerable support, further complicated the political landscape. His presence served as a potent reminder of the country's history of violent conflict and the unresolved grievances that continue to fuel political tensions (Human Rights Watch, 2021).

While the Ouattara administration touted a degree of political stability and successes in countering jihadist threats in the northern regions (Institute for Security Studies, 2022), this narrative of resilience often overshadowed the persistent concerns regarding human rights, the fairness of the electoral process, and the lack of genuine reconciliation between political factions (FIDH, 2021). Therefore, characterizing Ouattara's leadership as definitively "consolidated" neglects the significant contestation and underlyingFragilities that continued to define Côte d'Ivoire's political reality in 2022.

2.1 Political and Digital Landscape for Civic Engagement

The current political and digital landscape in Côte d'Ivoire is characterised by restrictions on civic space, with limited freedom of expression, association, and assembly. Digital platforms have become critical spaces for civic engagement but are monitored and censored through a

variety of methods that include legal restrictions, surveillance and self censorship. Recent political developments have introduced stringent laws targeting digital activism, reinforcing a hostile legal and regulatory framework. These laws including the more recent Law on Electronic Communication (2024), particularly Article 214, criminalise online dissent, impose heavy penalties for digital advocacy, and authorise surveillance measures that undermine privacy. These legal aspects are discussed in detail below.

Internet access varies widely across the population, with urban areas having higher connectivity rates and better digital literacy than rural regions. Rural areas face significant challenges due to inadequate infrastructure and limited access to digital education. The legal environment for digital rights is hostile, with governments exploiting vague cybersecurity laws to suppress online freedoms, monitor activists, and shut down internet services during politically sensitive periods.

The digital sphere has emerged as a critical battleground for civic engagement and human rights advocacy in Côte d'Ivoire. Social media platforms have become the primary tool for disseminating information, identifying human rights violations, and countering government propaganda. However, government restrictions and surveillance constantly threaten this digital space.

2.2 Challenges for CSOs in Côte d'Ivoire

Organisations in Côte d'Ivoire face challenges in utilising digital tools for democracy. Key informant interviewees conducted for this study, revealed surveillance, censorship of online content, prosecution threats of activists and journalists and possibility of internet shutdowns, even though this has not happened in recent years. In addition, key informant interviews also perceive some government policies such as mandatory data localisation and restrictions on encryption as tools that could be abused by the government to hinder CSOs' ability to use digital tools securely. Additionally, key informant interviews also revealed that many CSOs lack the technical expertise to protect themselves from cyber threats if they happen and limited funding restricts their ability to invest in advanced digital tools or hire skilled personnel. Apart from challenges associated with use of digital tools, some key informant interviews mention legal action or the threat of legal action as a hindrance to digital democracy work, with organisations fearing prosecution for online activities deemed critical of the government.

2.2.1 Digital Repression tactics

Internet Shutdowns: Authorities have disrupted internet connectivity before during politically sensitive periods, such as elections or protests. The last recorded internet shutdown was imposed during the 2020 presidential election and the 2021 protests against the constitutional amendment.

Surveillance and Censorship: Government agencies in Côte d'Ivoire use surveillance, monitoring online communications and censoring critical content. For instance, the legal framework, particularly the Cybercrime Law , grants authorities the power to monitor online activities under the guise of national security and combating cybercrime (Africa Center for Strategic Studies, 2022). This stifles freedom of expression and limits the ability of CSOs to operate effectively in the digital space.

2.2.2 Restrictive Policies

Government policies, such as data localisation laws and encryption restrictions, hinder secure communication and limit access to essential digital tools for CSOs. These policies make it difficult for CSOs to operate securely and effectively.

The 2013 Law on the Protection of Personal Data (Law No. 2013-450), has significant implications for digital democracy and the broader digital economy. The law mandates that the personal data of Ivorian citizens be stored and processed within the country, aiming to enhance data security, sovereignty, and control over sensitive information. While this fosters trust in digital systems and protects citizens' privacy, it also raises concerns about the accessibility and affordability of digital services, particularly for CSOs that may struggle to comply with the infrastructure requirements. For digital democracy, this could limit the ability of CSOs and activists to leverage global platforms for advocacy, as international tech companies might face barriers to operating freely.

The same law also regulates the use of encryption technologies to ensure data security and privacy, which can empower citizens, journalists, and activists to communicate securely and protect sensitive information from unauthorised access. However, the government's ability to mandate access to encrypted data under certain conditions, such as for national security purposes, raises concerns about potential overreach and surveillance.

While encryption safeguards freedom of expression and supports whistleblowing efforts, overly restrictive policies could undermine these protections. Balancing the need for security with the preservation of digital rights remains a key challenge, as overly stringent encryption controls could erode trust in digital platforms and hinder the growth of a transparent and participatory digital democracy in Côte d'Ivoire.

2.2.3. Capacity Gaps

Many CSOs lack the technical expertise and resources to protect themselves from cyber threats, conduct effective online advocacy, and utilise digital tools. This leaves them vulnerable to cyberattacks and limits their ability to fully engage in the digital space.

A key informant interviewee highlighted that during the 2020 presidential elections, some Ivorian CSOs involved in election monitoring and human rights reporting were targeted by cyberattacks, including phishing attempts and Distributed Denial of Service (DDoS) attacks, which disrupted their operations and compromised sensitive data. Without adequate cybersecurity measures, such as encryption tools or secure communication platforms, these organisations struggled to safeguard their information and maintain their online presence.

This vulnerability not only undermines their credibility but also discourages active participation in digital democracy, as fear of reprisals or data breaches may lead to self-censorship. Additionally, the lack of technical capacity limits their ability to leverage digital tools for campaigns, data analysis, and public engagement, reducing their impact in advocating for transparency, accountability, and social justice.

2.2.4 Funding Constraints

Conversations with key informants highlighted that many CSOs in Côte d'Ivoire are significantly constrained on financial resources to invest in secure technologies, sustain long-term advocacy campaigns, and hire skilled personnel. Many CSOs rely on outdated software and hardware, leaving them vulnerable to cyberattacks such as malware infections or data breaches. During the 2020-2021 political crisis, Ivorian CSOs working on human rights and election monitoring reported incidents where their systems were compromised, exposing sensitive information about activists and beneficiaries. Without the funds to purchase advanced cybersecurity tools or train staff in digital security best practices, these organisations remain exposed to ongoing threats. Additionally, the lack of financial resources limits their capacity to run sustained digital advocacy campaigns. Furthermore, the inability to hire skilled IT personnel or digital experts means that many CSOs rely on volunteers or overburdened staff with limited technical knowledge, further hampering their ability to innovate or adapt to the evolving digital landscape.

These challenges collectively weaken the role of CSOs in promoting digital democracy, as they are unable to fully leverage digital platforms to mobilise citizens, hold authorities accountable, or advocate for systemic change.

2.2.5 Legal and Regulatory Challenges

The legal and regulatory environment surrounding digital democracy and online freedom of expression has become increasingly restrictive, with vague laws and arbitrary enforcement posing significant challenges for CSOs, activists, and journalists. The 2019 law on cybersecurity and the fight against cybercrime (Loi relative à la cybersécurité et à la lutte contre la cybercriminalité) has been a focal point of concern. While the law was introduced to address cyber threats and protect national security, its broad and ambiguous language has been used to target online dissent. Provisions criminalising "offensive" or "insulting" content, terms that lack clear definitions, have enabled authorities to arrest and detain individuals for expressing critical opinions.

3.0 Examining the Shrinking Digital Civic Space in Côte d'Ivoire

3.1 Political and Digital Landscape

The legal and regulatory environment is increasingly hostile, with vague laws and arbitrary enforcement used to stifle online activism and restrict CSOs. This creates a climate of fear and self-censorship, limiting freedom of expression and hindering digital democracy work. For example, the 2019 law on cybersecurity and the fight against cybercrime has been used to arrest and detain activists and journalists for their online activities.

Although this is not widespread, authorities have the capacity to disrupt internet connectivity during politically sensitive periods, such as elections or protests, undermining advocacy efforts and limiting access to information. For instance, internet shutdowns were imposed during the 2020 presidential election and the 2021 protests against the constitutional amendment.

In May 2024, Côte d'Ivoire's Senate adopted the draft Electronic Communications Law after its adoption in the National Assembly. The law, particularly paragraph 3 of article 214, has been criticised for restricting press freedom. The article provides for prison sentences of up to five years and a fine of 10 million CFA francs (approximately 16,670 USD) for anyone found guilty of intercepting, disclosing, publishing or using the content of messages or revealing their existence.

Again in 2024, the Council of Ministers adopted an Order Ordinance 2024-368 on the organisation of civil society and the related ratification draft law, replacing the 1960 Law on Associations. The new regulations aim "to diligently align their organisational and operating methods with the current requirements of the fight against transnational organised crime. Article 48 of the ordinance obligates CSOs to submit annual activity reports, including CSOs that do not receive foreign funding. The Order also allows the administration to request special reports on ongoing projects;

Article 22 of the ordinance stipulates that CSOs can be dissolved through a decree issued by the Council of Ministers in case its activities "constitute a threat to public order and security, the integrity of the national territory and the republican form of the State, or which are likely to compromise social cohesion, provoke hatred between ethnic or religious groups, cause political unrest, discredit political institutions or their functioning, incite citizens to break the laws, and harm the general interest of the country". With this law, there is no possibility to appeal such a decision to dissolve an association as the Order also stipulates, in its article 53, that members of a dissolved CSO can be sentenced to a prison sentence between one and three years and fined 300,000 to three million CFA francs (approximately 500 to 5,000 USD) if they continue operating after it was dissolved, or if they knowingly organise a meeting with the members of the dissolved CSO.

3.2 Increased Surveillance and Censorship

The censorship of digital spaces in Côte d'Ivoire manifests through a variety of methods. Firstly, the legal and regulatory framework provides a foundation for restricting online expression. Laws such as the Cybercrime Law of 2013, with its broad definitions of cyber offenses, and the Penal Code,

which criminalises the dissemination of "false information" (MFWA, 2017), are wielded to target online dissent and critical voices. The more recent Law on Electronic Communication (2024), particularly Article 214 (ipi.media, 2024), introduces further restrictions on the publication of message content, raising concerns about its potential to stifle journalistic inquiry and encourage self-censorship. These legal instruments create an environment where online speech can be easily criminalised.

Surveillance also plays a role in the censorship apparatus. While concrete evidence of widespread systematic surveillance may be difficult to obtain publicly, the legal framework, particularly the Cybercrime Law , grants authorities the power to monitor online activities under the guise of national security and combating cybercrime (Africa Center for Strategic Studies, 2022). This potential for surveillance can lead to self-censorship as individuals become wary of expressing dissenting opinions online for fear of repercussions. The opacity surrounding the extent and nature of government surveillance contributes to a climate of uncertainty and apprehension among digital users, further constricting the space for free expression.

Although not a frequent occurrence, the potential for internet shutdowns remains a potent tool of censorship. The government possesses the technical capability to disrupt or block internet access during politically sensitive periods (Africa Center for Strategic Studies, 2022). While not consistently deployed, the threat of such shutdowns can have an effect on online mobilisation and the dissemination of information, effectively silencing digital spaces during critical times. This measure represents a drastic form of censorship, cutting off access to information and communication for entire populations.

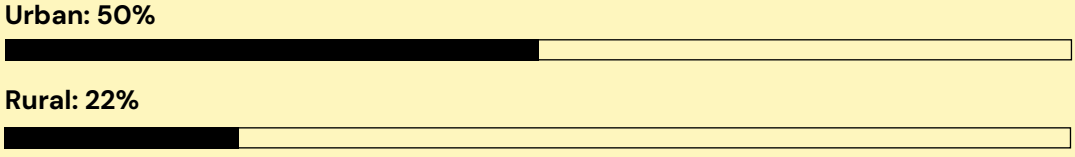
In addition, censorship occurs through less formal but equally impactful means such as content removal and blocking and intimidation and threats (Refworld, 2017). While specific instances of government-ordered content removal or website blocking may not always be publicly documented, the existing legal framework provides the authority for such actions. Furthermore, reports of journalists and bloggers facing intimidation, threats, and even physical security risks for their online activities contribute to a climate of fear and self-censorship. These tactics, though not codified in law as direct censorship, effectively silence critical voices and narrow the scope of acceptable online discourse.

3.3 Limited Access and Digital Literacy

The research noted that internet access remains uneven, with urban areas enjoying better connectivity than rural regions. This digital divide limits access to information and participation in online discussions for marginalised communities, particularly those in rural areas. The International Telecommunications Union (ITU) estimates that in Cote d'Ivoire urban-rural digital connectivity remains high.

Côte d'Ivoire - Urban and Rural Internet Penetration

Percentage of the population that uses the Internet in rural and urban areas



Note: Measurement methods vary by country.

2022

Data Source: ITU 2022

The digital divide is further worsened by the low digital literacy levels, especially in rural areas, compounding the challenges of accessing and utilising digital tools for civic engagement and democratic participation.

3.4 Policy Frameworks

The landscape of digital rights is shaped by a developing legal and policy framework alongside a growing digital penetration. The Constitution guarantees fundamental rights, which should extend to the online sphere, including the right to information and freedom of expression (Council of Europe, n.d.). To further solidify these rights in the digital age, Côte d'Ivoire has enacted specific legislation such as Law No. 2013-450 on the Protection of Personal Data (DataGuidance, n.d.) and Law No. 2013-451 on cybercrime. The Telecommunications/ICT Regulatory Authority of Côte d'Ivoire (ARTCI) plays a crucial role in overseeing the implementation of these laws and ensuring the protection of users' rights and privacy within the digital space.

The government has also outlined its ambitions for the digital sector through strategic documents like the National Digital Development Strategy (2021-2025). This strategy acknowledges the importance of strengthening data protection measures to foster a safer cyberspace and build digital trust. Furthermore, the National Cybersecurity Strategy (2021-2025) demonstrates a commitment to protecting the digital environment and safeguarding user data against increasing cyber threats (Digital Watch Observatory, n.d.). These strategic initiatives signal a growing recognition of the need to balance digital advancement with the protection of fundamental rights in the online realm.

Despite these positive steps, challenges and concerns regarding the practical application and enforcement of digital rights persist. Reports from international organizations highlight potential limitations on freedom of expression online and the risk of legal frameworks being used to stifle critical voices (Paradigm Initiative, 2023). A recent Electronic Communication Law has also raised concerns about its potential impact on press freedom (ipi.media, 2024). Moreover, the cost of internet access can still be a barrier for some segments of the population, contributing to a digital divide. Addressing these challenges and ensuring that legal and policy frameworks are effectively implemented and aligned with international human rights standards is crucial for fostering an open digital space in Côte d'Ivoire.

3.5 Legal Framework

The legal framework in Côte d'Ivoire poses significant obstacles to developing digital democracy. A range of restrictive laws and policies stifle online freedom of expression, impede access to information, and undermine the operations of CSOs. These measures have created a hostile environment for digital rights, limiting citizens' ability to engage in democratic discourse and online activism.

The Haute Autorité de la Communication Audiovisuelle et du Numérique (HACA) is tasked with regulating digital content, aiming to protect citizens' rights and ensure access to reliable information. However, the HACA's power to censor or restrict content deemed "political or social" creates a potential conflict of interest. The vague criteria for restricted content allow for subjective interpretations and potential political influence, raising concerns about transparency and accountability. Ultimately, this regulatory power, while designed to protect citizens, could be used to suppress dissent and limit access to diverse perspectives, thereby undermining democratic freedoms and open discourse within Côte d'Ivoire.

3.5.1 Cybersecurity and Fight Against Cybercrime Law

The 2019 Law on Cybersecurity was designed to combat cyber threats. While this presents a positive development the law contains vague and broad provisions weaponised to target activists, journalists, and dissenting voices. Individuals have been arrested and detained for posting content on social media deemed critical of the government. The law criminalises online dissent, imposing severe penalties such as hefty fines and imprisonment, which discourages open dialogue and fosters a culture of self-censorship.

Cybersecurity laws could potentially be exploited to justify disruption of internet services, however a total internet shutdown was last imposed in 2021 during the constitutional amendment protests. In 2022, a blogger was charged under cybersecurity laws for "spreading false information" after publishing a report on alleged government corruption. The vague nature of the law allowed authorities to interpret the offence broadly, leading to the blogger's prolonged detention without trial.

3.5.2 Data Localisation Laws

Cote d'Ivoire has passed data localisation laws that mandate that CSOs and other entities store sensitive data within the country. This provision makes it easier for the government to access and monitor locally stored information. This requirement compromises the ability of CSOs to protect their communications and data from state interference, mainly when working on sensitive issues such as human rights or governance. A local human rights organisation reported that state authorities intercepted its confidential communications with international partners after it was forced to store its data locally. This breach of privacy undermined the organisation's credibility and deterred potential collaborators.

3.5.3 Encryption Restrictions

Cote d'Ivoire restrictions on encryption technologies have the potential to hinder secure communication, leaving activists, journalists, and CSOs vulnerable to surveillance and hacking. Without robust encryption, these groups cannot safely share sensitive information or protect their digital assets from state and non-state actors. During a 2021 protest, activists attempting to coordinate logistics via messaging apps found their communications compromised due to government-mandated encryption restrictions. This led to the arrest of several organisers and disrupted the protest movement.

3.6 Impact of Repressive Laws and Policies on Civil Society

The cumulative effect of repressive laws and policies has a significant effect on digital democracy in Côte d'Ivoire. The deteriorating environment creates a chilling effect on freedom of expression, as individuals and organisations fear retaliation for voicing dissenting opinions online. Access to information is severely limited, particularly during critical moments such as elections or protests, when transparency is most needed. CSOs, which play a vital role in promoting democratic values and holding the government accountable, face immense challenges in carrying out their work due to surveillance, data vulnerabilities, and restricted communication channels.

The environment of fear and self-censorship stifles online activism and discourages citizens from participating in democratic discourse. This undermines the potential of digital platforms to serve as spaces for civic engagement and political mobilisation, ultimately weakening the foundations of democracy in the country. This scenario has led to several actions that impact digital democracy;

- **Targeting Journalists and Activists**

  In 2022, a judge placed a journalist and managing editor of the daily Le Panafricain, Barthélémy Téhin, under judicial supervision following a defamation complaint by the customs administration over the newspaper's reports on alleged corruption involving a customs officer. According to the Committee to Protect Journalists (CPJ), the judicial supervision was for an unspecified time pending further investigations by the judge.

- **Internet Shutdowns During Elections**

  The highly contested and controversial 2020 presidential election, occurring amidst violent protests, was marked by a complete internet shutdown. This shutdown severely limited access to crucial information, disrupting the work of election observers and CSOs tasked with monitoring the electoral process. The deliberate curtailment of online access, coupled with the backdrop of widespread unrest, significantly fueled allegations of electoral fraud and exacerbated already heightened tensions within the country.

- **Suppression of Protests**

  In 2024, authorities arrested 25 individuals on September 13th during a suppressed demonstration organised by the citizen platform Agir pour le peuple (AGIP), a coalition of 78 CSOs, which intended to protest escalating food, electricity costs, demanding an end to forced evictions and the demolition of informal settlements, and advocate for peaceful presidential elections following a ban on the protest. Subsequently, on September 17th, a court sentenced 16 of those arrested to six months' imprisonment for "disturbing public order," while the secretary-general of AGIP, Armand Krikpeu, faced further detention and awaited trial on serious charges, highlighting the challenges faced by civil society in exercising their rights to assembly and expression in Côte d'Ivoire despite constitutional guarantees, particularly concerning socio-economic grievances and political processes.

- **Surveillance of CSOs**

  A key informant interviewee working on governance and transparency issues reported that its emails and phone calls were monitored after it published a report critical of government spending. The organisation's staff faced harassment and intimidation, forcing it to scale back its operations.

4.0 CSOs Response and Adaptation Strategies

Despite the shrinking digital space in Côte d'Ivoire, CSOs have demonstrated resilience and adaptability in their efforts to promote digital democracy and navigate their challenges.

4.1 Embracing Secure Communication Tools

In an era where digital surveillance and censorship are increasingly prevalent, CSOs in Côte d'Ivoire have adopted a range of secure communication tools to protect their activities and ensure the safety of their members and partners. These tools help bypass censorship and safeguard sensitive information from potential surveillance.

CSOs in Côte d'Ivoire have turned to encrypted messaging apps like Signal and Telegram to ensure secure communication. These apps employ end-to-end encryption, making it nearly impossible for third parties to intercept or decipher messages. An interviewee mentioned that Signal is used effectively to coordinate activities and share sensitive information among its members. This has been particularly crucial in environments where state surveillance poses a significant threat to activists and human rights defenders. Signal's open-source nature and commitment to privacy have made it a trusted tool for CSOs globally.

In addition to messaging apps, CSOs have embraced secure platforms like Jitsi Meet and Zoom (with end-to-end encryption enabled) for virtual meetings, training sessions, and collaborative projects. These platforms minimise the risk of surveillance and interference, ensuring that sensitive discussions remain confidential. During the COVID-19 pandemic, many CSOs relied on these tools to continue their advocacy work while adhering to social distancing measures.

4.2 Coalition Building and Collaborative Advocacy

CSOs in Côte d'Ivoire have recognised the power of collective action in addressing digital rights issues. By forming partnerships and networks, they have amplified their impact and advocate more effectively for policy reforms. One notable example is the Coalition Ivoirienne pour les Droits Humains (CIDDH), a network of organisations working together to promote human rights and digital freedoms. By pooling resources and sharing information, these coalitions can more effectively tackle complex challenges. Collaborative efforts like these have been instrumental in addressing issues such as internet shutdowns and restrictive laws.

CSOs have also engaged in joint campaigns to raise awareness and advocate for change. This has also motivated the government to launch online campaigns raising public awareness on issues related to digital spaces. The **"#EnLigneTousResponsables"** campaign is one such national initiative launched by the government of Côte d'Ivoire in 2024 to cultivate a safe, respectful,

and secure digital environment for all Ivorian citizens (African Business, 2024). The campaign's primary intentions seek to raise awareness on both the advantages and potential risks associated with social media and digital tools. This includes fostering critical thinking skills regarding online information and promoting responsible online conduct (CFI, n.d.).

The campaign also intends to develop digital skills and knowledge among the populace, equipping them with the necessary tools to navigate the digital space safely and effectively. This involves training on identifying misinformation and understanding social media regulations (African Business, 2024). A significant focus is on combating misinformation, cyberbullying, cyber-harassment, and the spread of harmful rumors, encapsulated by the strong slogan "Stop au Sorcier Numérique" (Stop the Digital Sorcerer) (African Business, 2024).

This initiative is encouraging coming from the government and appears like the government is determined to instill a strong sense of digital responsibility among internet users, encouraging vigilance and the verification of information before dissemination (African Business, 2024). Interestingly, the campaign also engaged various stakeholders, including government bodies, international partners, media organizations, the private sector, local communities, and civil society groups (African Business, 2024). Furthermore, it incorporates monitoring mechanisms to assess its effectiveness and ensure long-term relevance (African Business, 2024).

"#EnLigneTousResponsables"

The **"#EnLigneTousResponsables"** campaign was launched in June 2024, with a pilot phase having been conducted in August 2023, allowing for refinement of the campaign's approach (African Business, 2024).

While it is still in its early stages, the initial reach and the sustained efforts suggest a positive trajectory towards achieving its goals of promoting responsible online behavior and combating misinformation in Côte d'Ivoire.

4.3 Public Awareness and Education

Raising public awareness about digital rights is a cornerstone of the work of CSOs in Côte d'Ivoire. These organisations have engaged communities and empowered individuals to navigate the digital landscape safely by focusing on storytelling and digital literacy. Some CSOs have effectively used storytelling to highlight the human impact of digital repression. The Actions pour la Protection des Droits de l'Homme (APDH) produced a series of short videos featuring individuals affected by internet shutdowns. These stories resonate with the public, making abstract issues like digital rights more relatable and urgent.

The National Council for Human Rights (CNDH) also plays a crucial role by monitoring and reporting on the human rights situation in Côte d'Ivoire, including digital rights violations. Their independent investigations and reports inform policy recommendations and advocacy efforts, influencing policy changes and legal reforms to protect digital right.

Digital Security and Literacy Training

The Ivorian Coalition of Human Rights Defenders, works to strengthen and protect the rights of human rights defenders, providing advice on digital security and training CSO members on digital security. Beyond the digital realm, the coalition addresses human rights violations across various sectors, including freedom of expression, assembly, and association. Through legal aid, advocacy, and capacity-building, they empower human rights defenders to operate more securely and effectively, contributing to a more robust defence of human rights in Côte d'Ivoire

The Ivorian Network for the Defence of Children's and Women's Rights (RIDDEF) utilises digital platforms and traditional community engagement to reach a wider audience, including those with limited internet access. Their online advocacy and educational campaigns raise awareness of digital rights and empower individuals to exercise them, while legal aid and support services provide crucial assistance to victims of online abuse and exploitation

The Convention de la Société Civile Ivoirienne (CSCI) focuses on capacity-building through training programs on ICT, cybersecurity, and the legal framework, equipping CSOs and citizens with the knowledge and skills to navigate the digital landscape safely and participate in online democratic processes. By fostering digital literacy and awareness, CSCI contributes to a more informed and engaged citizenry capable of leveraging digital tools for democratic participation and advocacy.

The Réseau des Professionnels de la Presse en Ligne de Côte d'Ivoire (REPPRELCI) have conducted digital literacy training programs to equip individuals with the skills to use digital tools safely and effectively. These programs are critical in a country where internet penetration is growing rapidly, but many users lack the knowledge to protect themselves online.

4.4 Engaging with Policymakers and International Actors

CSOs in Côte d'Ivoire have adopted evidence-based approaches to engage with policymakers and international actors, ensuring their advocacy efforts are grounded in data and research. The Centre Ivoirien de Recherches Economiques et Sociales (CIRES) published a report detailing the economic costs of internet shutdowns in Côte d'Ivoire. This report provided policymakers with concrete evidence of the negative impact of such measures, strengthening the case for policy reforms. CSOs have also collaborated with international organisations like Amnesty International and Access Now to raise awareness about digital rights violations in Côte d'Ivoire. These partnerships have helped bring global attention to local issues, increasing pressure on the government to respect digital freedoms.

4.5 Enhancing Digital Security Practices

Some CSOs in Côte d'Ivoire have implemented digital security measures, including VPNs and regular security audits to protect their data and communications. Using VPNs, CSOs can encrypt their internet traffic and mask their IP addresses, making it more difficult for surveillance entities to track their online activities. Additionally, regular security audits help identify vulnerabilities and ensure that systems are updated with the latest security protocols.

5.0 Digital Democracy Ecosystem Support to CSOs in Côte d'Ivoire

5.1 Ecosystem Support Systems

While Côte d'Ivoire faces challenges in advancing digital democracy, a support ecosystem exists to assist CSOs in navigating these obstacles. Among these support mechanisms include International donors who are actively funding initiatives aimed at strengthening civic space and supporting digital democracy projects globally. There are also capacity-building programs that provide training on digital security practices and advocacy strategies. However, these programs are often limited in scope and fail to reach all vulnerable organisations. The research showed that regional networks are underutilised due to limited awareness or fear of government surveillance. In addition, legal aid for organisations facing digital threats is scarce, and emergency response mechanisms are often reactive rather than preventive. The research also noted that CSO-Tech company engagement remains inconsistent, with some companies providing tools or platforms for advocacy work while others sometimes comply with government demands that could potentially undermine civil society's efforts, such as content takedowns requests..

5.1.1 International Donors - Funding and Capacity-Building

International donors are pivotal in supporting digital democracy initiatives in Côte d'Ivoire. Organisations like the European Union provide funding and capacity-building programs to strengthen civic space and promote digital rights. Smaller or rural-based CSOs often struggle to access funding due to complex application processes and limited outreach. This creates disparities in resource allocation, leaving many organisations underserved.

5.1.2 Capacity-Building Programs

Capacity-building programs are critical for equipping CSOs with the skills to operate safely and effectively digitally. Organisations like Access Now and CIVICUS have conducted workshops on digital security and advocacy strategies in Côte d'Ivoire. Access Now has trained journalists and human rights defenders to protect their digital footprints.

5.1.3 Regional Networks: Collaboration and Knowledge Sharing

Regional networks, such as the West Africa Internet Governance Forum (WAIGF), provide platforms for CSOs to collaborate, share knowledge, and coordinate efforts on digital rights issues. The WAIGF brings stakeholders from across West Africa to discuss internet governance and advocate for policies that protect digital rights. Another regional initiative is the West Africa Civil Society Institute (WACSI) established by the Open Society Initiative for West Africa (OSIWA) to strengthen digital capacity and Safety. It empowers CSOs in the region with essential skills to navigate the digital world securely.

5.1.4 Tech Company Engagement: Tools and Platforms

Tech companies have the potential to support digital democracy by providing tools and platforms that facilitate advocacy and communication. These partnerships have enabled CSOs to amplify their voices and reach broader audiences. Tech companies' engagement is inconsistent, and many comply with government demands that undermine digital rights, such as content takedowns or data access requests. This creates challenges for CSOs striving to maintain their online presence and protect user privacy.

5.2 Creative Approaches to Navigate Restrictive Landscape

CSOs in Côte d'Ivoire have demonstrated remarkable ingenuity in navigating the challenges of the shrinking digital space, continuing their vital work in promoting digital democracy. Their innovative strategies ensure the survival of their advocacy efforts, empower communities and strengthen digital rights.

5.2.1 Leveraging Digital Tools for Advocacy and Awareness

CSOs have effectively used platforms like Facebook, Twitter, and Instagram to run impactful advocacy campaigns. A good case in point is Internews and its local partners implemented a three-pronged strategy to counter hate speech in Côte d'Ivoire. Firstly, a dedicated four-member observatory monitored 9,925 Facebook profiles, groups, and pages from September 2020 to January 2022, producing 67 weekly reports. These reports revealed a correlation between political issues and hate speech, with Facebook pages as the primary dissemination platform, increased sexist hate speech against women in the news, and a shift to social media during elections.

Internews also provided media literacy training to young social media users in Abidjan and Grand-Bassam in 2020, focusing on online hate speech and its effects. Students' resulting drawings were refined by cartoonists for a public awareness campaign.

Lastly, in 2021, launched a national awareness campaign targeted both the public and local political leaders, educating them about hate speech, its consequences, and the need for responsible public discourse. This recognised the political class as a key source of hate speech and disinformation.

Online Petitions and Surveys: Platforms like Change.org and Google Forms have become essential for CSOs to gather public opinion and mobilise support. The Ivorian League for Human Rights (LIDHO) launched an online petition calling for the repeal of restrictive cyber laws, garnering over 10,000 signatures. This data-driven approach provides CSOs with evidence to support their advocacy efforts and demonstrates widespread public backing for digital rights.

Creative Content; To make complex digital rights issues accessible, CSOs produce engaging content such as short videos, infographics, and blog posts. A good case is the Internews "Carton Rouge," a weekly 10-minute radio and online segment that confronts hate speech launched in 2022, (Internews, 2024). The program educates audiences about its dangers, featuring diverse perspectives, including victims, activists, artists, politicians, psychologists, and traditional leaders. Listeners are directed to the Internews Civilia Facebook page for more information. Broadcast in prime time, "Carton Rouge" airs for a year on Radio de la Paix (24 cities), Radio Al Bayane (the nation's most popular station), and ~20 partner stations nationwide. It is also available as a Facebook video and regional debates are hosted by radio partners.

5.2.2 Circumventing Censorship and Surveillance

To bypass government-imposed censorship, CSOs like the Côte d'Ivoire Internet Society Chapter have trained partners to use VPNs. This allows them to access blocked websites and social media platforms, ensuring uninterrupted communication and information sharing. For example, during the 2020 elections, VPNs enabled CSOs to report on elections.

6.0 Gaps and Recommendations

Strengthening the support ecosystem for digital democracy in Côte d'Ivoire requires a multi-faceted approach addressing funding, capacity, networking, legal aid, and grassroots community engagement.

Sustainable Funding Mechanisms

Current funding models often favour larger, urban-based CSOs, leaving smaller and rural organisations struggling to access resources. Multi-year funding programs provide stability, allowing these organisations to plan strategically and invest in long-term projects. Simplified grant application processes reduce administrative burdens, especially for organisations with limited staff and resources. Consideration should be given to funding diverse types of digital democracy initiatives, from digital literacy training to platform development and online advocacy campaigns. Increased and more equitable funding empowers smaller CSOs to engage in digital democracy initiatives, broadening participation and ensuring diverse voices are heard. Long-term funding also fosters sustainability and allows for more impactful projects.

Expanded Capacity-Building Programs

Training programs should cover critical areas like digital security (protecting data, preventing cyberattacks, online safety), effective advocacy strategies (online campaigning, social media engagement, digital storytelling), and digital literacy (using online tools, accessing information). These programs should also be accessible to rural organisations, potentially through online training materials in local languages, and travel subsidies.

Digital security training is vital in protecting CSOs from online threats and ensuring their work can continue. In addition, reaching rural organisations ensures that digital democracy efforts are inclusive and address the needs of all communities.

Regional Networks

Regional networks like the WAIGF play a crucial role in fostering collaboration, knowledge sharing, and advocacy. Strengthening these networks involves providing resources for coordination, communication, and joint initiatives. Stronger regional networks also facilitate collaboration and amplify the voices of CSOs working on digital democracy. They can provide platforms for sharing best practices, coordinating campaigns, and collectively addressing regional challenges. International monitoring and support mechanisms create a safety net for CSOs facing digital threats and promote a culture of accountability.

Legal Aid Mechanisms

Proactive legal aid programs go beyond reactive assistance after a legal issue has arisen. They involve providing preventative legal advice, training CSOs on digital rights and legal frameworks, and developing resources to help them navigate legal challenges. Timely access to legal assistance is crucial, as delays can have serious consequences. This may involve establishing a network of lawyers specialising in digital rights, creating legal clinics, and providing legal representation in court. Timely access to legal assistance ensures that CSOs can effectively respond to legal threats and protect their interests. Without adequate legal support, CSOs may be silenced or forced to self-censor due to fear of legal repercussions.

Tech Company Engagement

Tech companies play a significant role in shaping the digital space. Encouraging them to adopt transparent, rights-respecting policies is essential for protecting digital democracy. This could involve advocating for policies that respect freedom of expression, privacy, and access to information. Fostering partnerships between CSOs and tech companies can lead to the development of tools and platforms that support digital democracy while safeguarding user rights. This could involve collaborative projects on platform governance, content moderation, and data privacy.

Partnerships with CSOs can lead to the development of innovative solutions that address the challenges of digital democracy. Without engagement from tech companies, efforts to promote digital democracy may be undermined by harmful practices and policies.

6.1 Conclusion

This case study explored the dynamics of digital democracy in Côte d'Ivoire, examining the challenges and opportunities faced by CSOs operating in a restrictive environment. Côte d'Ivoire exemplifies the growing influence of digital technologies on civic engagement. However, the study reveals a shrinking digital civic space characterised by restrictive legal frameworks, including ambiguous cybersecurity laws, data localisation requirements, and encryption limitations, which are often used to suppress online dissent and hinder CSO activities. The 2019 cybersecurity law and subsequent legislative amendments have exacerbated this environment, fostering a climate of fear and self-censorship. Additionally, they are reports of government agencies engage in surveillance, monitor online communications, and censor critical content, undermining freedom of expression.

Disparities in internet access, particularly in rural areas, combined with low digital literacy levels, further exacerbate the digital divide and limit participation in online democratic discourse. As a result, Ivorian CSOs face numerous obstacles, including, restrictive policies, capacity gaps in digital security and technical expertise, funding shortages, and complex legal and regulatory barriers.

The study underscores the resilience and adaptability of Ivorian CSOs, which have developed innovative strategies to navigate this constrained environment. These strategies include adopting secure communication tools such as encrypted messaging apps, secure meeting platforms, and VPNs to protect their communications and circumvent censorship. CSOs are also building coalitions and engaging in collaborative advocacy to amplify their impact and advocate for policy reforms related to digital rights.

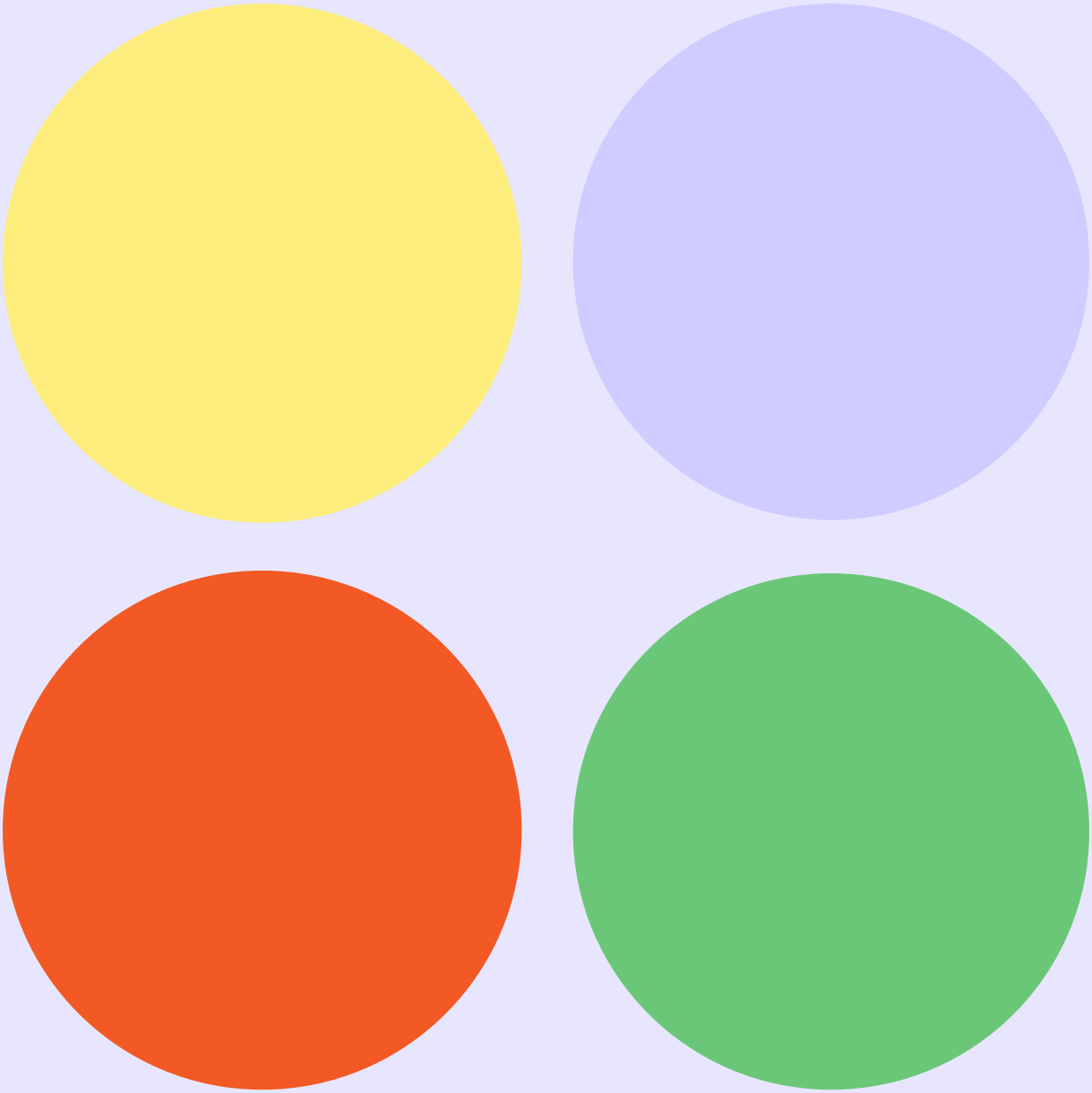
Public awareness and education initiatives play a central role in their efforts, with CSOs leveraging storytelling, digital literacy training, and public campaigns to empower individuals to safely navigate the digital landscape. Furthermore, CSOs are engaging with policymakers and international actors, employing evidence-based approaches and collaborating with global organisations to highlight digital rights violations. To enhance their resilience, CSOs are also strengthening their digital security practices by implementing measures such as VPNs and conducting regular security audits to safeguard their data and communications.

The report also assesses the existing support ecosystem for digital democracy in Côte d'Ivoire, which includes international donors, capacity-building programs, regional networks, and engagement with technology companies. However, this ecosystem faces some limitations. Key findings reveal uneven access to funding, with smaller, rural-based CSOs often struggling to secure resources. While capacity-building programs are essential, their reach is often limited, leaving many vulnerable organisations underserved. Regional networks remain underutilised due to limited awareness. Legal aid for organisations facing digital threats is scarce, and emergency response mechanisms tend to be reactive rather than proactive.

The study proposes several recommendations to strengthen the digital democracy ecosystem

in Côte d'Ivoire. These include establishing sustainable funding mechanisms, such as multi-year funding programs with streamlined application processes, to support diverse digital democracy initiatives and ensure equitable access for smaller and rural CSOs. Expanding capacity-building programs to deliver comprehensive training on digital security, advocacy strategies, and digital literacy, with a focus on accessibility for rural organisations, is also critical. Strengthening regional networks by providing resources to foster collaboration, knowledge sharing, and advocacy on digital rights issues is another key recommendation. Developing accessible legal aid mechanisms, including proactive legal advice, digital rights training, and timely legal representation for CSOs facing digital threats, is equally essential. Finally, fostering meaningful engagement with technology companies by promoting transparent, rights-respecting policies and encouraging partnerships between CSOs and tech companies to develop tools and platforms that support digital democracy is vital.

Nurturing a thriving digital democracy in Côte d'Ivoire requires sustained and collaborative efforts from all stakeholders to create an enabling environment where technology empowers citizens and strengthens democratic institutions.



Annexes

References

1. Access Now, 2020, Côte d'Ivoire elections: keep internet on to protect democracy, https://www.accessnow.org/press-release/cote-divoire-elections-protect-democracy/
2. African Business, 2024,. "Online All Responsible": A New Chapter Against Disinformation. African Business. https://african.business/2024/06/apo-newsfeed/online-all-responsible-a-new-chapter-against-disinformation
3. Africa Center for Strategic Studies, 2022, Deluge of Digital Repression Threatens African Security. https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/
4. Bertelsmann Stiftung, 2024, BTI 2024 Country Report on Cote d'Ivoire,
5. Cebul, C. and Pinckney, J., 2021, Facial Recognition Technology and the Right to Privacy in the Age of Digital Authoritarianism.
6. CFI. (n.d.). Project to combat disinformation in Ivory Coast. CFI. https://cfi.fr/en/project/project-combat-disinformation-ivory-coast
7. CIPESA, 2022, Digital Authoritarianism and democratic participation in Africa, https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief-.pdf
8. CIVICUS, n.d., CIVICUS Monitor, Cote d'Ivoire
9. CIVICUS, 2023, People Power Under Attack 2023, CIVICUS.
10. DataGuidance, n.d.,Ivory Coast, Jurisdictions, https://www.dataguidance.com/jurisdiction/ivory-coast
11. Council of Europe, n.d., Côte d'Ivoire, Octopus Cybercrime Community https://www.coe.int/en/web/octopus/-/cote-ivoire
12. Digital Watch Observatory, n.d., Côte d'Ivoire, Digital Watch Observatory https://dig.watch/countries/ivory-coast
13. Digital Watch Observatory, n.d., Ivory Coast's cybersecurity strategy (2021-2025) https://dig.watch/resource/ivory-coasts-cybersecurity-strategy-2021-2025
14. Feldstein, S., 2021. The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press
15. Frantz, E., Kendall-Taylor, A. and Wright, J., 2020. Digital repression in autocracies. Varieties of Democracy Institute Users Working Paper (27), pp.1-22
16. Freedom House, 2023, Côte d'Ivoire - Media Landscape
17. Freedom House 2023, Freedom on the Net
18. Freedom House, 2024, Countries and Territories,
19. Human Rights Watch, 2020, World Report 2020: Côte d'Ivoire, Human Rights Watch, https://www.hrw.org/world-report/2020/country-chapters/cote-divoire
20. Internews, 2024, In Côte D'Ivoire, We Raise the Red Card to Fight Online Hate Speech, https://internews.org/story/in-cote-divoire-we-raise-the-red-card-to-fight-online-hate-speech/
21. ipi.media, 2024, Côte d'Ivoire Electronic Communication Law raises concern for press freedom, https://ipi.media/alerts/cote-divoire-electronic-communication-law-raises-concern-for-press-freedom/
22. Jose-Ignacio Torreblanca, 2023, Social Networks and Democracy: Problems and Dilemmas of Regulating the Digital Ecosystem
23. Keremoğlu, E., Feldstein, S., and Reisinger, J., 2020, Repression's Digital Toolkit 2.0. Journal of Democracy, 31(4), pp. 105-118.
24. Lungu, P. C, 2024., The impact of digital transformation on democracy. A study case on# rezist movements. https://www.researchgate.net/publication/383018968_The_impact_of_digital_transformation_on_democracy_A_study_case_on_rezist_movements
25. Ministry of Foreign Affairs of Denmark, 2024, DIGITAL DEMOCRACY INITIATIVE

26. MFWA, 2017, MFWA Submission To The Third UPR Of Côte D'ivoire Freedom Of Expression Developments since second UPR https://Uprdoc.Ohchr.Org/Uprweb/Downloadfile.Aspx?Filename=6453&File=Englishtranslation

27. Paradigm Initiative,2023, LONDA – DIGITAL RIGHTS AND INCLUSION IN AFRICA REPORT, https://paradigmhq.org/wp-content/uploads/2023/06/Cote-divoir-Londa-2022.pdf

28. Poisson M, 2024, How Civil Society Uses Digital Tools to Increase Accountability in Education, UNESCO International Institute for Educational Planning (IIEP), https://educationoutloud.org/how-civil-society-uses-digital-tools-increase-accountability-education

29. Refworld, 2017, Freedom Of The Press 2017 - Côte D'ivoire, https://Www.Refworld.Org/Country,,,,Civ,,5a4cd502d,0.Html

30. Ronak Gopaldas, 2019, The South African Institute of International Affairs (SAIIA), Digital Dictatorship versus Digital Democracy in Africa

31. United States Agency for International Development (USAID), 2021, Digital Democracy: How to Prevent and Reverse Democratic Backsliding in the Digital Age

32. Wainscott, C., Owen, T., and Crabtree, C., 2021, Rights-Respecting Technology: A Framework to Protect and Empower Civil Society in the Digital Age. CIVICUS and the Engine Room.

33. West, H., 2023, Digitalisation and democracy. Gütersloh: Bertelsmann Stiftung.

34. Youngs, R. and Breuer, A, 2022, Digital Authoritarianism and Democratic Participation in Africa. Gütersloh: Bertelsmann Stiftung.Weinhardt, C., Fegert, J., Hinz, O. et al., 2024, Digital Democracy: A Wake-Up Call

Ecosystem support to CSOs in Côte d'Ivoire

Country	Name of Organization	Description
Côte d'Ivoire	Oxfam	International NGO working on poverty alleviation and social justice.
	CARE International	Humanitarian organisations are fighting global poverty and providing emergency relief.
	Save the Children	It focuses on children's rights and providing humanitarian aid.
	ActionAid	Works to fight poverty and injustice around the world.
	Handicap International	Supports people with disabilities and vulnerable populations in conflict zones.
	European Union	Provides financial resources, capacity-building programs, and collaborative opportunities.
	USAID	Supports economic growth, health, education, and democracy.
	French Development Agency	Promotes economic and social development through loans and grants.
	GIZ	Implements development projects on behalf of the German government.
	UNDP	Works on poverty reduction, democratic governance, and crisis prevention.
	UNICEF	Focuses on children's rights and well-being.
	UN Women	Promotes gender equality and women's empowerment.
	Open Society Initiative for West Africa (OSIWA)	Supports civil society activities through grants and capacity-building initiatives.
	Ford Foundation	Supports social justice and human rights initiatives.
	Mastercard Foundation	Focuses on education and youth development in Africa.
	Friedrich Ebert Stiftung (FES)	German political foundation that promotes social democracy and supports civil society organisations.
	Konrad Adenauer Stiftung (KAS)	German political foundation that promotes Christian democracy and supports civil society organisations.
	National Democratic Institute (NDI)	American non-profit organisation that supports democratic institutions and practices around the world.
	International Republican Institute (IRI)	American non-profit organisation that supports democratic institutions and practices around the world.
	Interpeace	Supports peacebuilding and conflict resolution initiatives.
	Search for Common Ground	Works to prevent and transform conflict through dialogue and mediation.
	Amnesty International Côte d'Ivoire	Focuses on human rights research, advocacy, and campaigns.
	Human Rights Watch Côte d'Ivoire	Monitors and reports on human rights abuses.
	Ligue Ivoirienne des Droits de l'Homme (LIDHO)	Ivorian Human Rights League advocating for human rights and democratic freedoms.
	Réseau Ivoirien pour la Défense des Droits de l'Enfant et de la Femme (RIDDEF)	Network defending the rights of children and women in Côte d'Ivoire.
	Convention de la Société Civile Ivoirienne (CSCI)	Platform of Ivorian civil society organisations working on various social and political issues.

Defining Digital Democracy and Digital Repression

This section presents the theoretical definition of Digital democracy and digital repression. Digital democracy signifies using digital technologies to bolster and enhance democratic values and practices. It is a dynamic concept encompassing a range of activities and principles to foster citizen participation, transparency, and accountability in the digital age. The critical components of digital democracy include but are not limited to the following:

- **Online Participation:** Citizens can engage in political processes and decision-making through digital platforms, such as online voting, e-petitions, public consultations, and online forums for deliberation and debate. The "Digital Democracy" (2022) report highlights that digital media can facilitate dialogue between governments and citizens, improve institutional trust, and enable engagement between diverse groups.
- **Access to Information:** The availability and accessibility of information online enable citizens to make informed decisions and hold their governments accountable, which includes access to government data, public records, and independent media sources. The "Digital Authoritarianism and Democratic Participation in Africa (2022) policy brief emphasises the importance of access to information for meaningful citizen participation. In Côte d'Ivoire, for instance, the lack of a developed Access to Information law, as noted in the "Côte d'Ivoire - Media Landscape" report (2023), hinders the free flow of information and limits citizens' ability to make informed decisions.
- **Transparency:** Digital technologies enhance government transparency by enabling the publication of official data, live-streaming of parliamentary sessions, and disclosure of public expenditures. These technologies facilitate greater openness and visibility of government actions and decision-making processes. The Bertelsmann Transformation Index (BTI) 2024 Country Report on Côte d'Ivoire criticises Côte d'Ivoire's lack of transparency in budget planning and implementation, particularly regarding the military's economic enterprise.
- **Accountability:** Citizens' ability to hold their elected officials and government institutions accountable for their actions through digital means, such as online monitoring of government performance, reporting corruption, and demanding transparency. The "Digital Authoritarianism and Democratic Participation in Africa" (2022) notes that digital tools can be used for "naming and shaming" tactics, holding government actors accountable.
- **Digital repression** is "using information and communications technology to surveil, coerce, or manipulate individuals or groups to deter specific activities or beliefs that challenge the state" (Feldstein, 2021, p. 25). Regimes can use digital repression to maintain power and, more generally, to undermine democratic values and human rights worldwide. To counter this, rights-respecting technology frameworks are viewed as opportunities to strengthen democratic values in digital societies (Wainscott et al., 2021).

Digital Democracy
Initiative