UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Southern Africa Regional Office

PROTECTING HUMAN RIGHTS AND CIVIC SPACE ONLINE

INTRODUCTION

The Internet has enabled an expansion of civic space and more people to claim and defend their fundamental rights, regardless of frontiers. These rights are guaranteed under the Universal Declaration of Human Rights and other United Nations Human Rights treaties*.

Despite lockdown restrictions, the COVID-19 pandemic proved that digital technology can help maintain meaningful communication and the enjoyment of human rights, including the right to education, access to information, health, participation in public affairs, and the right to express one's opinions. As a result, the internet helped maintain democracy, peace, and development during times of crisis.

Conversely, the advancement in digital technologies worldwide has also led to new forms of online threats. As a result of these threats, hate speech is exacerbated and discrimination, hostility, or violence is incited. Harmful disinformation is being spread in an unprecedented manner, cybercrimes and cyberattacks are occurring, and patterns of discrimination and exclusion are being echoed online.

States have sought to respond to these and other challenges by regulating the online space and online content. In doing so, they often have adopted overly broad regulations, and practices, that put at risk the enjoyment of human rights by internet users, in particular their rights to privacy, to freedom of expression and information and to freedom of peaceful assembly and association or the right to participate in public affairs. Among the multiple means implemented by States, are the regulation of the online content, large-scale surveillance using digital tools, as well as shutting down the internet or restricting access to it.

This advocacy brief gives an overview of the current landscape in respect of the three main challenges for human rights in online civic space in Southern Africa: (1) online content regulation and censorship (2) surveillance (3) connectivity/internet disruptions. It also makes recommendations on how to address associated risks in accordance with international human rights law.

Digital technologies have expanded opportunities for people to defend human rights, but also pose new risks.

See page 5: Status of ratification of core human rights treaties related to online civic space

United Nations Office of the High Commissioner for Human Rights Regional office for Southern Africa, Pretoria, South Africa
Email: ohchr-rosa@un.org
Website: https://www.ohchr.org/en/countries-and-territories/africa-region/un-human-rights-southern-africa
Tel: +27 12 354 8684

Image credit: Pexels/Monstera; Logo: OHCHR

Image credit: Pexels/Ketut-Subiyanto

ONLINE CIVIC SPACE IN SOUTHERN AFRICA: KEY CHALLENGES

1. CONTENT REGULATION AND CENSORSHIP

States have an interest to ensure that the internet advances, rather than undermines public participation and debate, including through regulation. In some countries, legislation has been passed to regulate online content to fight terrorism, harmful disinformation or cybercrimes, citing protection of national security, public order, public health or morals, which are grounds for restricting freedom of expression, association and assembly, provided those restrictions conform to the strict tests of proportionality and necessity. At times, this legislation has been passed under emergency tabling procedures, or without meaningful consultation of the public and other stakeholders, thus failing to adhere to international human rights standards on the right to participation and the principles of legality. Meaningful participation makes decision-making more informed and sustainable, and public institutions more effective, accountable and transparent. This in turn enhances the legitimacy of States' decisions and their ownership by all members of society[2].

Some of the legislation gives wide-ranging powers to the Government to restrict online communications based on overly broad concepts of national security or public safety. In other instances, the laws include overly broad and subjective definitions of terrorism, defamation, hate speech, sedition, treason, or they criminalize vague concepts of "disinformation", "online promotion of extremism", "cybercrime", etc., which make it extremely difficult to determine with reasonable certainty what kind of conduct, both online and offline, is prohibited.

Such laws create room for arbitrary decisions and unlawful violations of human rights and fundamental freedoms, in particular of expression and information. In practice, they have been used by some States to silence voices deemed critical of the authorities, in particular human rights defenders, activists, and journalists, and members of political opposition. These actors have been prosecuted for their online communications and punished severely, including with prison sentences which are clearly disproportionate. While the courts of some jurisdictions have struck down the offence of criminal defamation, most countries in the sub-region have not repealed such laws.

Vague and broad definitions of crimes and offences or grounds to restrict online content, are likely to contravene the principles of legality, necessity and proportionality, leading to blunt censorship, both by removing content and prosecuting their authors – which ends up undermining the ability of civil society groups to expose violations of their rights.

> The Human Rights Committee has ***expressed concern*** over provisions of some press laws in the sub-region that criminalize publication of a text or image that is offensive to individuals, and the existence of defamation provisions in criminal laws, which may be used to ***silence dissenting voices*** and ***penalize statements*** made by members of the media[3].

Image credit: Pexels/Christina Morillo

2. SURVEILLANCE

State institutions are frequently given the possibility to collect and store personal data based on laws providing law enforcement authorities with a broad range of emergency and national security related powers which may result in surveillance of targeted individuals or groups, both online and offline. The global proliferation of hacking tools has led to an unprecedented level of targeted and covert surveillance of digital devices by State institutions, trying to protect against cybercrime. However, this surveillance may end up monitoring communications of journalists, opposition political figures and human rights defenders.

These broad surveillance powers and tools, coupled with insufficient legal safeguards or judicial oversight, create a risk of abuse and violations of fundamental rights in particular the right to privacy and the right to freedom of expression. Surveillance has a chilling effect for the entire society and is particularly problematic for human rights defenders, journalists and opposition leaders. Surveillance is also associated with violent attacks, arbitrary arrests and detention, torture and extra-judicial killings.

In spite of the benefits of encryption as a key enabler of privacy and security online and for safeguarding fundamental rights, some countries restrict the use of encryption. In Southern Africa, some decrees and laws give licence to States to monitor citizens' online activities and include provisions that grant authorities unfettered powers to compel companies to facilitate access to encrypted user data for security agencies and weaken encryption technologies. Weakening of encryption is also used in tandem with traceability requirements, where messages can be traced back to the originator using their IP address. This poses a serious threat to security of human rights defenders, civil society and journalists and other online users.

While some courts in the sub-region have declared provisions of certain laws relating to the interception of communications unconstitutional as they do not provide safeguards to protect the right to privacy, other laws on interception of communications do not provide for judicial oversight over authorities and telecommunication companies exercising surveillance powers.

While there are not universally agreed definitions, ***Disinformation*** is increasingly considered to be "information that is false and deliberately created and shared to harm a person, social group, organisation or country".

Misinformation, is "information that is false but not created or shared with the intention of causing harm".

Mal-information, is "information that is based on reality, used to inflict harm on a person, social group, organisation or country". Mal-information may include sharing sensitive or personal details that may harm the reputation of others without a public interest justification.

Source: Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training, UNESCO, 2018

Image credit: Pexels/Carlos Cruz

3. CONNECTIVITY AND INTERNET SHUTDOWNS

Internet shutdowns are measures taken by a government, or on its behalf, to disrupt access to, and the use of, information and communications systems online. They include actions that limit the ability of a large number of people to use online communications tools, either by restricting internet connectivity at large or by obstructing the accessibility and usability of services that are necessary for interactive communications, such as social media and messaging services. Access to the internet is widely recognized as an indispensable enabler of a broad range of human rights. It is not only essential for freedom of expression, but, as digitalization advances, it is also central to the realization of the rights to education, to freedom of association and assembly, to participate in social, cultural and political life, to health, to an adequate standard of living, to work and to social and economic development, among others.

Despite global commitments to promote internet connectivity, governments continue to order internet shutdowns, in some cases repeatedly. Between 2016 and 2021, the #KeepItOn coalition reported 931 internet shutdowns in 74 countries[7]. In Southern Africa, internet shutdowns have occurred in a number of States, including during periods of heightened political tensions, such as the periods surrounding elections or during large-scale protests/civil unrest, and during the COVID-19 pandemic. In some instances the shutdowns have been ordered pursuant to legislation on cybersecurity or interception of communications or without relying on legislation at all or they rely on too broad concepts of public interest, national security, public order and curtailment of spread of false information/incitement[8].

While internet shutdowns deeply affect many human rights, they most immediately affect freedom of expression and access to information[9]. Restrictions on the right to freedom of expression are only permissible when they meet the requirements set out by international human rights law[10].

Any restrictions must be provided by law and must be necessary and proportionate to achieve one of the following legitimate goal: protection of national security or of public order, or of public health or morals, or respect of the rights or reputations of others.

The Human Rights Committee has clarified that the law relied upon to restrict freedom of expression must be precisely formulated to enable an individual to regulate her or his conduct accordingly, and it must be made publicly available.

The Human Rights Committee has clarified that the law relied upon to restrict freedom of expression must be ***precisely formulated*** to enable an individual to regulate her or his conduct accordingly, and it must be made publicly available.

When States impose internet shutdowns or disrupt access to communications platforms, the legal foundation for their actions is often unstated. When laws are invoked, the applicable legislation can be vague or overly broad, which would fail to meet the requirements. For example a law referring to public order or national security that does not specifically address the surrounding circumstances and conditions for internet shutdowns is not sufficiently precise. The Human Rights Committee has further indicated that, national security cannot be used especially where national security is proclaimed as a means to supress of human rights[11].

Given their indiscriminate reach and broad impacts, internet shutdowns very rarely meet the fundamental requirements of necessity and proportionality. Their adverse impacts on numerous rights often extend beyond the areas or periods of their implementation, rendering them disproportionate, even when they are meant to respond to genuine threats[12].

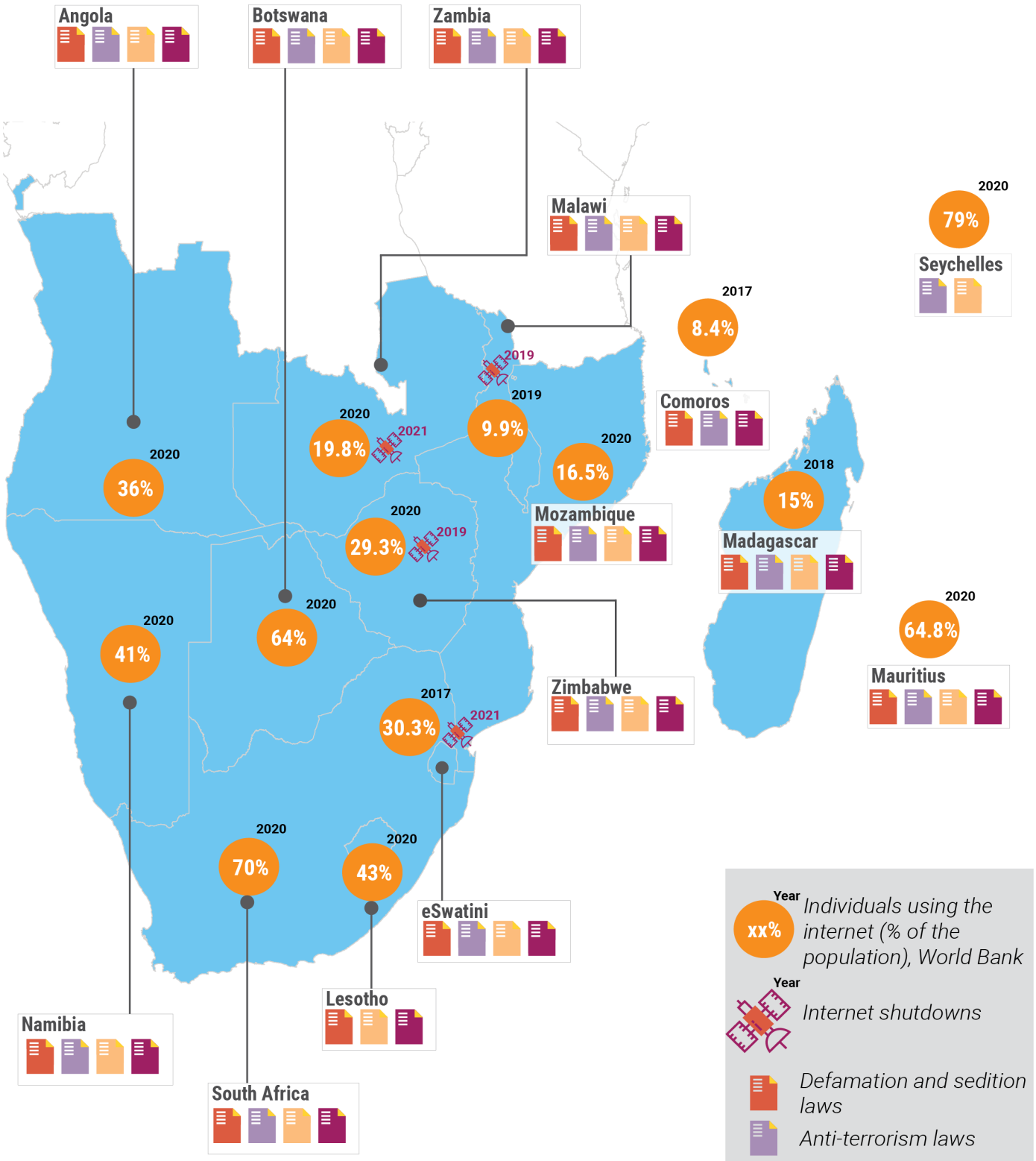
Image credit: Pexels/Monstera

STATUS OF RATIFICATION OF CORE HUMAN RIGHTS TREATIES RELATED TO ONLINE CIVIC SPACE

Human Rights Treaty	Countries who have ratified treaty*
International Covenant on Civil and Political Rights (ICCPR)	Angola, Botswana, eSwatini Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
International Covenant on Economic, Social and Cultural Rights (ICESCR)	Angola, eSwatini Lesotho, Madagascar, Malawi, Mauritius, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)	Angola, Botswana, Comoros, eSwatini Lesotho, Madagascar, Malawi, Mauritius Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
Convention on the Rights of Persons with Disabilities (CRPD)	Angola, Botswana, Comoros, eSwatini Lesotho, Madagascar, Malawi, Mauritius Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
International Convention on the Elimination of all Forms of Racial Discrimination (ICERD)	Angola, Botswana, Comoros, eSwatini Lesotho, Madagascar, Malawi, Mauritius Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT)	Angola, Botswana, Comoros, eSwatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
Convention on the Rights of the Child (CRC)	Angola, Botswana, Comoros, eSwatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Zambia, Zimbabwe
International Convention for the Protection of All Persons from Enforced Disappearance (ICPPED)	Lesotho, Malawi, Seychelles, Zambia
International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (ICRMW)	Lesotho, Madagascar, Malawi, Mozambique, Seychelles

**As at November 2022*

LEGISLATION REGULATING ONLINE CIVIC SPACE IN SOUTHERN AFRICA



CONCLUSIONS AND RECOMMENDATIONS

People around the world are witnessing impressive technological developments, as well as innovations that improve people's lives and boost economies. However, they are also experiencing how digital tools can be turned against them, exposing them to new forms of monitoring, profiling and control, including by the unprecedented levels of personal data collection[14]. Ensuring respect for and protection of fundamental rights in the online space is essential for the full enjoyment of all human rights in the digitized societies. **With this in mind:**

STATES ARE REQUIRED TO ENSURE THAT:

- Their legal framework especially the laws governing cybersecurity and cyber-crime surveillance and counterterrorism laws and ensuring compliance with international human rights norms and standards[15].
- Defamation laws comply with article 19 (3) of the ICCPR and they do not serve in practice to stifle freedom of expression. Care should be taken to avoid excessively punitive measures and penalties, and where relevant, States should place reasonable limits on the requirement for a defendant to reimburse the expenses of the successful party. States should also consider the decriminalization of defamation[16].
- Any attempt to regulate online content should be clearly and narrowly prescribed in law, be proportional and necessary for the protection of "national security", "public order" and "public health or morals" or "respect of the rights or reputation of others".
- Online crimes and offenses should be clearly defined. In particular those related to terrorism and national security should not be used or interpreted to justify steps to silence political opponents, oppress peaceful protests, prosecute human rights defenders and hamper the work of journalists. Disinformation should not be addressed with criminal law.
- Measures such as cutting off access to the internet and telecommunications services, in particular in the context of elections or during times of civil unrest are ceased[17].
- Strong encryption and anonymity is promoted and protected, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, rather than on law enforcement agencies[18].
- Ensure that any interference with the right to privacy, including restrictions to access and use of encryption technology and surveillance of the public, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality and non-discrimination, and does not impair the essence of that right[19].
- The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising the right to peaceful assembly and association, both in physical spaces and online is prohibited[20].

BUSINESS/ TELECOMMUNICATION COMPANIES SHOULD:

- Take all possible lawful measures to prevent internet shutdowns and, if the shutdown should nevertheless proceed, prevent or mitigate to the extent possible adverse human rights impacts; exhaust domestic remedies to challenge shutdown requests and implement shutdown requests narrowly, in the most human rights-preserving way, with the goal of keeping communications channels as open as possible; and take all lawful measures to enable the full disclosure of information about the interferences[21].
- Take all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses or violations[22].
- Conduct due diligence and impact assessment to prevent or mitigate any adverse impact on human rights resulting from their operations, products or services[23].
- Take effective measures to ensure transparency of their policies and practices, including the application of their terms of service and of computation-based review processes, and respect due process guarantees[24].

CIVIL SOCIETY IS ENCOURAGED TO:

- Expand and improve data collection on – and documentation of digital threats to – the rights of expression and opinion: in particular with respect to legal developments, network disruptions, surveillance, and online harassment and disinformation campaigns[25].
- Share knowledge, promote standards for data collection, and collaborate with other stakeholders in these efforts[26].
- Engage in the process of understanding digital threats to civic space and developing effective responses to threats[27].
- In relation to internet shutdown, CSOs should reinforce collaborative efforts to prevent, detect, study and respond to Internet shutdowns[28].
- Ensure that digital security and digital literacy are at the core of their organization's activities and promote access to circumvention tools, paying due attention to their safety, accessibility and affordability[29].

ENDNOTES

1. UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on reinforcing media freedom and the safety of journalists in the digital age,* A/HRC/50/29
2. United Nations Guildelines for States on the Effective Implementation of the Right to Participate in Public Affairs. Page 3.
3. Universal Human Rights Index-Human Rights Recommendations https://uhri.ohchr.org/en/ document/1475e6c7-c190-47e8-af99-a170bac8f437 and https://uhri.ohchr.org/en/document/14d60002-48f0-4336-84da-438647414981
4. United Nations Human Rights Council, *Report of the Office of the High Commissioner for Human Rights on the right to privacy in the digital age,* A/HRC/51/17, para 21.
5. United Nations Human Rights Council, *Report of the Office of the High Commissioner for Human Rights on Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights,* A/HRC/50/55, para 4
6. A/HRC/50/55, para 7
7. See #KeepItOn: Fighting internet shutdowns around the world (accessnow.org)
8. Southern Africa Litigation Centre & Media Institute of Southern Africa, Report: Navigating litigation during internet shutdowns in Southern Africa Page 10 (Accessed here: https:// www.southernafricalitigationcentre.org/wp-content/uploads/2019/08/SALC-Internet-Shutdown-Guide-FINAL.pdf
9. A/HRC/50/55, para 9
10. See article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR).
11. Human Rights Committee, general comment No. 37 (2020), para. 42.
12. A/HRC/50/55, para 59
13. A/HRC/51/17, para 2
14. Ibid.
15. United Nations Human Rights Council, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and association, AHRC/41/41, para 73(c).*
16. Human Rights Committee General Comment 34 on Article 19 ICCPR on freedoms of opinion and expression, para 47
17. A/HRC/41/41, para 74
18. A/HRC/41/41, para 73(d)
19. A/HRC/51/17, para 56
20. A/HRC/41/41, para 76
21. A/HRC/50/55, para 69
22. A/HRC/41/41.
23. A/HRC/50/29, para 125.
24. A/HRC/41/41, para 87
25. Ibid, para 94
26. Ibid, para 94
27. Ibid, para 95
28. A/HRC/50/55 Para 71
29. Ibid, para 93