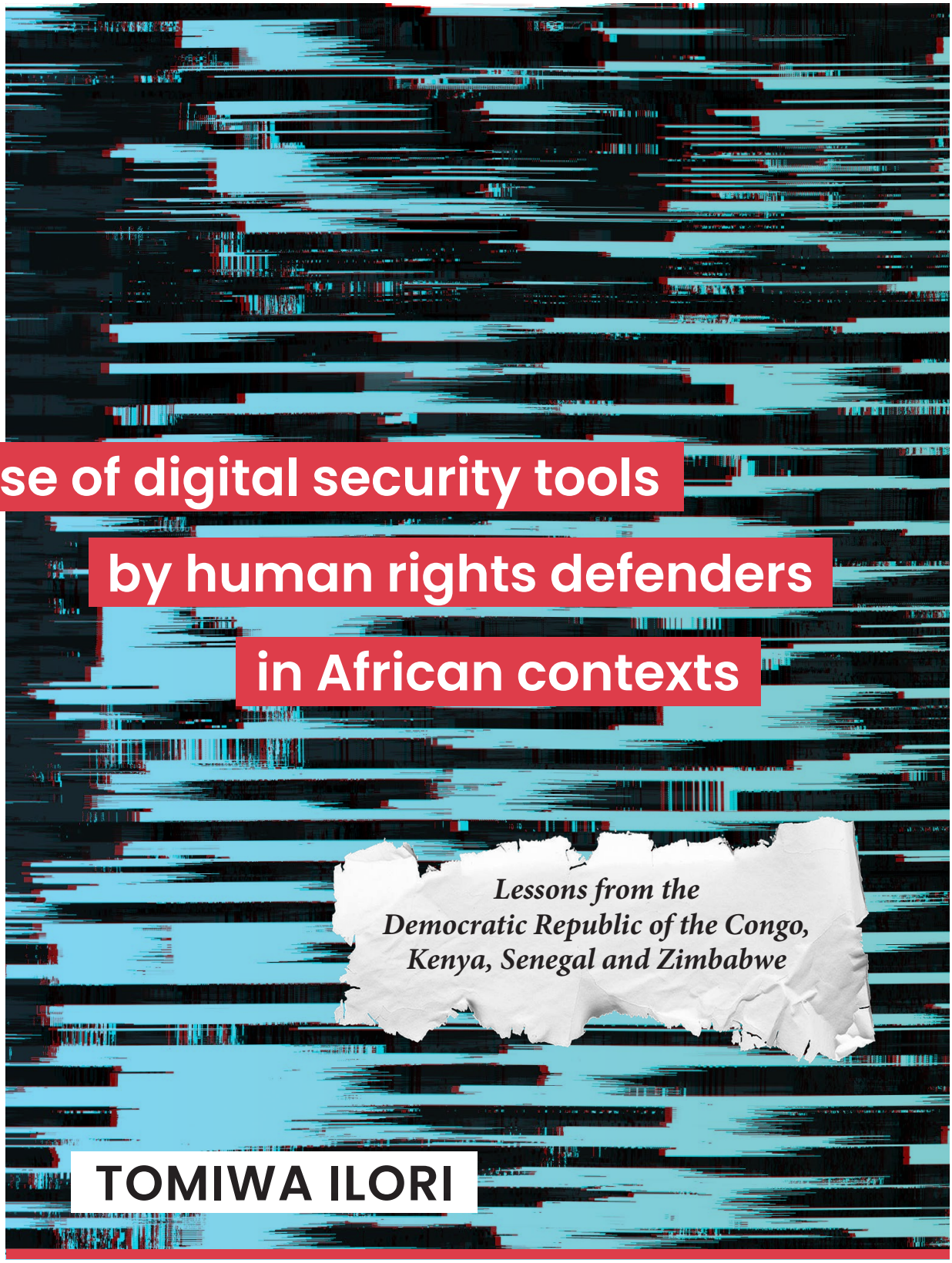


Use of digital security tools by human rights defenders in African contexts

Lessons from the Democratic Republic of the Congo, Kenya, Senegal and Zimbabwe

TOMIWA ILORI

A report of a fellowship project
supported by Open Technology Fund and hosted by HURIDOCS

OPEN TECHNOLOGY FUND

huridocs

Use of digital security tools by human rights defenders in African contexts

Lessons from the Democratic Republic of the Congo, Kenya, Senegal and Zimbabwe

TOMIWA ILORI

A report of a fellowship project
supported by Open Technology Fund
and hosted by HURIDOCS.

July 2025

Table of contents

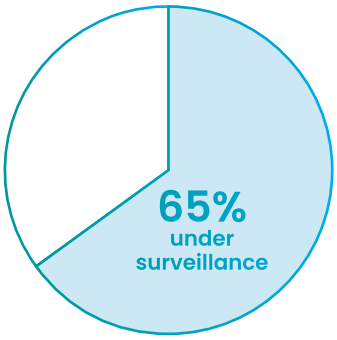
Summary

This report examines how human rights defenders (HRDs) in African contexts including the Democratic Republic of the Congo, Kenya, Senegal, and Zimbabwe use digital security tools to protect themselves in high-risk political and digital environments. It uses existing literature, survey responses and interviews with HRDs and developers of digital security tools to highlight key challenges such as pervasive state surveillance, limited access to digital infrastructure, low digital literacy, and the technical complexity of existing digital security tools. However, both HRDs and tools developers expressed strong interest in collaboration, co-design, and digital security training to improve usability. The report recommends a comprehensive approach to digital security which includes co-design, continuous training support, and reform to ensure HRDs are capacitated and protected in their work.

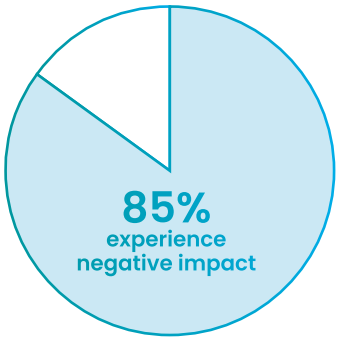
Key findings of the report

KEY FINDING 1

Pervasive state surveillance threatens HRDs' safety and work



65% of HRDs believe they are under surveillance by state actors



85% of HRDs believe political environment has a negative impact on their work

The majority (65%) of HRDs across the countries studied believe they are under surveillance by state actors and 85% of HRDs believe that their political environment has a negative impact on their work. This surveillance is not only real but also perceived which

creates a climate of fear that leads to self-censorship, psychological stress, and operational constraints. These threats are compounded by repressive laws and government practices that criminalise dissent and restrict internet freedoms, which severely impact HRDs' ability to advocate safely and effectively.

KEY FINDING 2

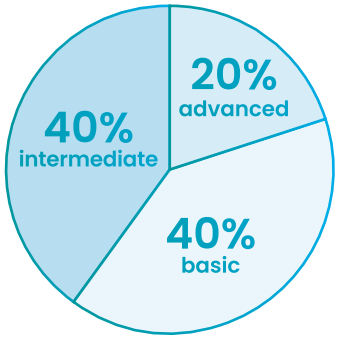
Limited access to digital infrastructure and resources hampers tool adoption

More than half of HRDs in these countries face significant digital and systemic infrastructural challenges such as unreliable internet, high data costs, outdated devices, and power outages. These issues are pronounced in rural and conflict-affected areas where connectivity is poor or non-existent. Women human rights defenders (WHRDs) in these regions face additional gender-based forms of violence such as doxing, sexual harassment, and non-consensual sharing of intimate images. As a result, many HRDs rely on platforms like WhatsApp and Facebook due to their accessibility. The lack of affordable, secure, and locally adapted digital tools limits HRDs' ability to protect themselves and their work in high-risk political environments.

KEY FINDING 3

Digital security skills and usability gaps limit effective tool use

The report reveals that only 20% of HRDs possess advanced digital security skills, while 40% have basic and intermediate skills. This skills gap, combined with the technical complexity of many digital security tools leads to underutilisation of digital security tools. Some of these tools are often seen as too complicated without proper training and access to affordable and reliable internet. Peer adoption is also low which makes secure communication difficult. WHRDs in rural areas face compounded challenges due to limited access to training and digital literacy. These findings demonstrate the need for user-friendly, context-specific tools and continuous capacity-building efforts.



20% of HRDs possess advanced digital security skills, while 40% have basic and intermediate skills

KEY FINDING 4

Tool developers are willing to engage but face challenges

Most (90%) digital security tool developers express strong interest in collaborating with HRDs even though most HRDs have never interacted with a developer. Developers mentioned that they face constraints such as limited funding and small teams, which hinder their ability to localise tools and respond to user feedback effectively. Language barriers and lack of structured engagement platforms further limit collaboration. In spite of these challenges, developers are committed to improving usability, expanding language support, and building tools that reflect the realities of HRDs in African contexts.

90% of digital security tool developers express strong interest in collaborating with HRDs

KEY FINDING 5

Strong demand for co-design, training, and inclusive digital security ecosystems

The digital security risks that HRDs face have become complex. This is why they articulated a clear need for regular and hands-on training programmes tailored to varying skill levels and local contexts. They emphasised the importance of tools that are affordable, offline-capable, and available in local languages. There is also a strong desire for co-design opportunities with developers to ensure tools are relevant and responsive. Both HRDs and developers support the creation of multi-stakeholder platforms for continuous collaboration. These findings point to the need for a comprehensive and inclusive approach to digital security that goes beyond technology to include continuous training and support.

Glossary of key terms

Civil society
refers to organisations and individuals that operate independently from the government to advocate for human rights and public interests.

Co-design
refers to a participatory approach where end-users are actively involved in the design process to ensure tools meet their needs.

Digital infrastructure
refers to the essential technologies and systems such as internet access, devices, electricity, and digital tools that enable human rights defenders to operate safely and effectively online.

Digital literacy
refers to the ability to use digital tools and technologies to find, evaluate, create, and communicate information.

Digital security tool
refers to any technical or non-technical resource designed to help human rights defenders protect their digital information, communications, and activities from unauthorised access, surveillance, or attack.

Digital security
refers to the protection of digital information and the systems that store and transmit it from unauthorised access, use, disclosure, disruption, modification, or destruction.

Encryption
refers to the process of converting information into a secret code to prevent unauthorised access, ensuring confidentiality and data integrity.

Human rights defenders

refers to individuals or groups who act to promote or protect human rights and may include activists, journalists and digital security trainers

Localisation

refers to the process of adapting digital tools and content to meet the language, cultural, and contextual needs of specific user communities.

Metadata

refers to data that provides information about other data, such as the time and location a file was created or modified.

Multi-dimensional

refers to the interconnected and overlapping nature of risks, challenges, and impacts that human rights defenders face in digital environments.

Open-source

refers to software with source code that anyone can inspect, modify, and enhance.

Ransomware

refers to a type of malware that encrypts a victim's files and demands payment to restore access.

Social engineering

refers to the manipulation of individuals into divulging confidential information or performing actions that compromise security.

Spyware

refers to malicious software designed to enter a device, gather data, and forward it to a third party without the user's consent.

Surveillance

refers to the monitoring of behaviour, activities, or information for the purpose of information gathering, influencing, managing, or control.

Threat modelling
refers to the process of identifying, assessing, and prioritising potential threats to digital security in order to develop mitigation strategies.

Usability
refers to the ease with which human rights defenders can use a tool or system to achieve a specific goal effectively and efficiently.

Virtual private network refers to a service that encrypts your internet traffic and routes it through a remote server, masking your Internet Protocol (IP) address and enhancing online privacy.

1. Introduction

IN DOCUMENTING ABUSES, HRDs HAVE BECOME VICTIMS THEMSELVES.

Safeguarding those who defend human rights whether through physical protection or digital security, is an ongoing and vital effort. However, in African contexts, human rights defenders (HRDs) are facing mounting challenges. As they advocate for justice, expose violations, and support vulnerable communities, they are subjected to surveillance, censorship, and threats, both online and offline. In documenting abuses, HRDs have become victims themselves.[1] While their role as documenters has gained more recognition, there remains limited attention on the risks they face simply for being HRDs in the context of pervasive and intrusive unlawful surveillance in politically repressive environments.

Unlawful surveillance has become pervasive today because most surveillance tools have the capacity to automatically extend the scope of data and information collection. These tools are also intrusive because they require almost no interaction to violate the privacy and other human rights of their targets. Additionally, these tools have the capacity "to collect and deliver an unlimited selection of personal and private data (along with data of any contact with which a target of surveillance interacts)."[2] Digital attacks are carried out in many ways including unlawful interception of private communication and information, spyware attacks, ransomware use, and social engineering threats by malicious actors.[3]

In recent years, studies conducted on the prevalence of state surveillance practices across African contexts show that African governments invest heavily in the purchase and use

1 UN General Assembly. (2020). Report of the Special Rapporteur on the Situation of Human Rights Defenders, Mary Lawlor (UN Doc A/75/165). https://documents.un.org/doc/undoc/gen/n20/185/66/pdf/n2018566.pdf?OpenElement (accessed Aug. 7, 2024); American Friends Service Committee. (2024). Digital Safety & Security in Africa. https://afsc.org/sites/default/files/2024-06/africa-report-reformatted.pdf (accessed Aug. 7, 2024).

2 Amnesty International. (July 23, 2021). Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector. https://www.amnesty.org/en/documents/doc10/4491/2021/en/ (accessed Aug. 7, 2024).

3 Amnesty International Security Lab. Digital Security Resource Hub for Civil Society. https://securitylab.amnesty.org/digital-resources/ (accessed Aug. 8, 2024).

of surveillance technologies such as digital devices, software and systems that monitor and gather information about individuals' communications and activities.[4]While most African governments justify these practices as a need to protect national security and combat crimes, studies reveal that such practices equate to abuse of power that violate international human rights standards required to conduct lawful and targeted surveillance. This is because these practices are usually without adequate legal and security safeguards which often result in violations of human rights of at-risk actors including HRDs in politically repressive and low-resource environments in African contexts.[5] Given this background, this report explores how HRDs in four countries: the Democratic Republic of the Congo, Kenya, Senegal, and Zimbabwe use digital security tools to protect themselves and what more needs to be done by relevant stakeholders to support them.

Dakar, Senegal (Pierre Laborde / Shutterstock.com)

4 Abdulrauf, L. A. (2018). The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa. African Human Rights Law Journal, 18, 365–391; Collaboration on International ICT Policy for East and Southern Africa (CIPESA). (2023). Compelled Service Provider Assistance for State Surveillance in Africa: Challenges and Policy Options. https://cipesa.org/wp-content/files/Compelled_Service_Provider_Assistance_for_State_Surveillance_in_Africa_Policy_Brief.pdf (accessed Aug. 8, 2024); Hebert, K. (Oct. 4, 2023). Rising Digital Surveillance Threatens Africa's Democratic Progress. ISS African Futures. https://futures.issafrica.org/blog/2023/Rising-digital-surveillance-threatens-Africas-democratic-progress (accessed Aug. 7, 2024); Roberts, T., Gitahi, J., Allam, P., Oboh, L., Oladapo, O., Appiah-Adjei, G., Galal, A., Kainja, J., Phiri, S., Abraham, K., Klovig Skelton, S., & Sheombar, A. (2023). Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia. Institute of Development Studies. https://doi.org/10.19088/IDS.2023.027 (accessed Aug. 7, 2024); Small Media, CIPESA, Centre for Intellectual Property and Information Technology Law, & Defend Defenders. (2017). Safeguarding Civil Society: Assessing Internet Freedom and the Digital Resilience of Civil Society in East Africa. https://cipesa.org/wp-content/files/briefs/Assessing_Internet_Freedom_and_the_Digital_Resilience_of_Civil_Society_in_East_Africa_2017.pdf (accessed Aug. 10, 2024).

5 Dube, H., Simiyu, M. A., & Ilori, T. (2020). Civil Society in the Digital Age in Africa: Identifying Threats and Mounting Pushbacks. Centre for Human Rights & CIPESA. https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Civil_society_in_the_digital_age_in_Africa_2020.pdf (accessed Aug. 9, 2024).

2. Methodology

This report adopts a mixed-methods approach by integrating both quantitative and qualitative research methods to investigate how HRDs in African contexts use digital security tools, and how tool developers can better respond to their needs. The qualitative component involved a review of existing literature including academic articles, civil society reports, and other relevant publications to contextualise the digital security landscape for HRDs in selected African contexts. It also included follow-up key informant interviews with selected survey participants consisting of HRDs and tool developers to deepen insights where needed. The quantitative component consisted of survey responses from 41 HRDs across the Democratic Republic of the Congo, Kenya, Senegal, and Zimbabwe, as well as developers of 11 digital security tools namely Awala, Butter Box, Lethro, Mobile Surveillance Monitor (MSM), Shira, SMSWithoutBorders (RelaySMS and DekuSMS), TAILS, Tella, Tor VPN, and Uwazi.

MORE THAN HALF OF THE HRD RESPONDENTS WERE WOMEN.

The surveys and interviews were conducted between October 2024 and April 2025 and contained mostly open-ended questions covering topics such as political and surveillance environments, access to digital infrastructure, tool usability, and developer feedback mechanisms.[6] More than half of the HRD respondents were women, and 12 local civil society organisations from the focus countries were engaged to support dissemination of the research findings in each of the country contexts. Additionally, a meeting was organised for HRDs, tool developers and local organisations to discuss the major findings and share their feedback.

All quotes from respondents in this report are anonymised to protect their identities. Descriptors such as country, gender, or location are used only when necessary to provide context.

6 Appendices.

3. Overview of HRD's adoption of digital security tools in African contexts

The risks faced by HRDs have become complex.[7] This is because before the advent of supercharged digital surveillance, physical surveillance of HRDs was the most common. Today, real and perceived threats of surveillance combined with physical surveillance cause great risks to the safety and security of HRDs across African contexts. Due to evolving new technologies such as facial recognition, biometrics and artificial intelligence, HRDs face unprecedented levels of surveillance risks when these technologies are combined. In a research that identifies the threats faced by civil society in African contexts, it was noted that not only do HRDs face state-sponsored unlawful surveillance, laws relating to online freedoms and in particular interception of communications are also crafted in ways that violate the rights of HRDs.[8] These laws usually require internet service providers (ISPs) to provide state actors with backdoor access to personal communications while also limiting the use of privacy-enhancing technologies such as encryption, anonymisation and pseudonymisation.

DUE TO EVOLVING NEW TECHNOLOGIES HRDs FACE UNPRECEDENTED LEVELS OF SURVEILLANCE RISKS.

In another collaborative research by more than 80 journalists and 17 media organisations in 10 countries, it was revealed that the Israeli spyware company, NSO Group had potential clients from 11 countries including Morocco, Togo and Rwanda.[9] The research further revealed that pervasive and intrusive surveillance technologies such as the Pegasus spyware were used to target more than 50,000 phone numbers including those of HRDs. As noted in the research, not only are these targets fearful for their safety, their family also became potential victims of surveillance which led to reluctance to engage with those who might be victims of surveillance. Research focusing on the chilling effects of surveillance in

7 UN Human Rights Council. (2024). Report of Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, Clément Nyaletossi Voule (UN Doc A/HRC/56/50).

8 Dube, Simiyu, & Ilori (n 5).

9 Amnesty International (n 2).

Uganda and Zimbabwe shows that HRDs interviewed as potential subjects of both real and perceived surveillance emphasised their inability to work and organise.[10]

In addition, a community-driven initiative that maps surveillance technology and spyware used to target and suppress HRDs revealed that out of the 55 African countries, at least one form of surveillance technology can be detected in 26 countries.[11] The top three countries where most surveillance technologies are found are Nigeria (9), Kenya (8) and South Africa (8).

Most HRDs believe that they are under state-sponsored surveillance as a result of their work which makes them vulnerable and puts them in fear of their safety.[12] There is also anecdotal evidence that African governments are conducting unlawful surveillance of HRDs across African contexts.[13] Oftentimes, these surveillance tools are purchased by African governments from foreign private companies under the pretext of ensuring national security but they are usually used to monitor HRDs.[14]

10 Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2024). The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe. Journal of Human Rights Practice, 16(1), 397–412. https://doi.org/10.1093/jhuman/huad020 (accessed June 30, 2025).

11 The countries are Angola, Botswana, Cameroon, Comoros, Democratic Republic of Congo, Côte d'Ivoire, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Ghana, Guinea, Kenya, Madagascar, Mali, Mauritania, Mauritius, Nigeria, Rwanda, South Africa, Sudan, Tanzania, Togo, Uganda, Zambia and Zimbabwe. See Surveillance Watch https://www.surveillancewatch.io (accessed Aug. 12, 2024).

12 Pan-African Human Rights Defenders Network. (2017). State of African Human Rights Defenders 2016. https://africandefenders.org/wp-content/uploads/2018/12/StateofHRD2016EnglishFinal-2.pdf (accessed Aug. 12, 2024); Defenders Coalition. (2020). Perception Survey: Impact of Communication Surveillance on Human Rights Defenders in Kenya. https://defenderscoalition.org/reports/4912-2/ (accessed Aug. 12, 2024).

13 Munoriyarwa, A., & Mare, A. (2022). Digital Surveillance in Southern Africa: Policies, Politics and Practices. Palgrave Macmillan; Caldero, R. (Oct. 10, 2023). Predator Spyware Allegations Rattle Angola. The Rio Times. https://www.riotimesonline.com/predator-spyware-allegations-rattle-angola/ (accessed Aug. 19, 2024); Rozen, J. (July 14, 2021). Botswana Police Use Israeli Cellebrite Tech to Search Another Journalist's Phone. Committee to Protect Journalists. https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/ (accessed Aug. 17, 2024); Mwere, D. (April 24, 2019). MPs Slap 10-Year Ban on OT-Morpho. Business Daily Africa. https://www.businessdailyafrica.com/bd/economy/mps-slap-10-year-ban-on-ot-morpho-2247754 (accessed Aug. 15, 2024).

14 Roberts & others (n 4).

Most HRDs have noted that in addition to the violation of their human rights as a result of unlawful surveillance, they suffer both physical and mental health challenges. Therefore, in most instances, whether real or perceived, surveillance threats have chilling impacts on HRDs and their work.

These risks do not only show the political dimensions of unlawful surveillance through the repression of civil rights including the rights to privacy, expression, association and assembly, it also points to the negative impacts of surveillance on socio-economic rights as it affects the rights of HRDs including those with disabilities to physical and mental health and their right to work.[15] Another major impact of surveillance on HRDs is that in order to be safe from harassment and physical arrests, they are forced to watch what they say, which ultimately leads to self-censorship. WHRDs have also been victims of existing negative social stereotypes that perceive women as social actors who can only be seen but not heard.[16] This contributes to targeted surveillance of WHRDs and therefore increases their safety risks of technology-facilitated online gender-based violence such as hate speech, doxing, sexual harassment, non-consensual sharing of intimate images.[17]

A MAJOR IMPACT OF SURVEILLANCE ON HRDs IS THAT THEY ARE FORCED TO WATCH WHAT THEY SAY, WHICH ULTIMATELY LEADS TO SELF-CENSORSHIP.

Most HRDs who work in African countries do so in challenging contexts.[18] These difficult contexts are as a result of hostile political environments where preventive and

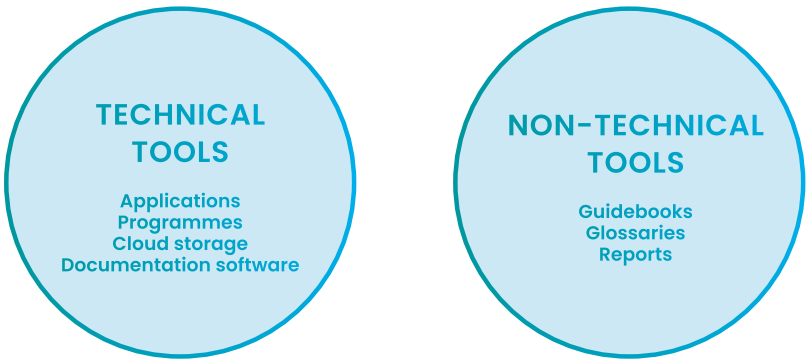
15 Nah, A. M., Jones, M., & Unal, M. (2024). Strengthening the Inclusion, Protection and Wellbeing of Human Rights Defenders with Disabilities. Protection International. https://www.protectioninternational.org/news/new-publication-on-strengthening-the-inclusion-protection-and-wellbeing-of-human-rights-defenders-with-disabilities/ (accessed Aug. 15, 2024).

16 Women Human Rights Defenders International Coalition (WHRD-IC). (2015). Gendering Documentation: A Manual For and About Women Human Rights Defenders. https://www.omct.org/site-resources/legacy/whrd_ic_gendering_documentation_manual_1_2020-12-11-144541.pdf (accessed Aug. 14, 2024); Protection International. (2014). Protecting Your Life, My Life, Our Lives: A Guide to Women Human Rights Defenders in Kenya. https://www.protectioninternational.org/wp-content/uploads/2022/12/Online-NO4A-GUIDE-TO-WHRDS-IN-KENYA-010915.pdf (accessed Aug. 14, 2024); SafeSisters is a digital security project focused on the protection of women human rights defenders in 17 countries including fellows from Democratic Republic of Congo, Kenya and Senegal. 13 out of the 17 countries are also based in Africa. See SafeSisters, https://safesisters.org/resources/ (accessed Aug. 14, 2024).

17 Rudi International, & Association for Progressive Communications (APC). (2014). Human Rights in the Digital Context and the State of Civic Space in the Democratic Republic of Congo. https://www.apc.org/sites/default/files/UPR_DRC.pdf (accessed Aug. 14, 2024).

18 Unwanted Witness. (2025). Surveillance/Spyware: An Impediment to Civil Society, HRDs and Journalists in East & Southern Africa. https://www.unwantedwitness.org/wp-content/uploads/2025/06/Report-06.06.2025-FINAL.pdf (accessed June 30, 2025).

protective digital security tools are out of reach.[19] These digital security tools include technical and non-technical tools. The technical tools include applications, programmes, cloud storage, and human rights documentation software designed to keep HRDs safe from unauthorised access to their personal information and communications.[20] Non-technical tools may be described as guidebooks, glossaries, and reports that provide accessible information for HRDs on how to minimise their exposure to digital risks.[21] As noted by a UN Human Rights Council report, there is a need to develop and provide



clear digital security tools and training dedicated for civil society, online activists, and HRDs.[22] To address this need, the digital security of HRDs in repressive political and underserved environments needs to be treated as a continuous process. Unfortunately, resources that seek to provide digital security assistance for HRDs are usually published once and are rarely developed and updated to accommodate the dynamic challenges presented by new technologies to HRDs' safety.[23] This presents a problem where existing digital security tools are unable to meet the dynamics of today's pervasive surveillance

19 Public International Law & Policy Group, The Engine Room, & HURIDOCS. (2020). Human Rights Documentation by Civil Society – Technological Needs, Challenges, and Workflows. https://huridocs.org/wp-content/uploads/2022/08/PILPG-HRDocSolutions-AssessmentReport.pdf (accessed Aug. 5, 2024).

20 The Engine Room. (2018). Technology Tools in Human Rights. https://library.theengineroom.org/humanrights-tech/#introduction (accessed Aug. 5, 2024).

21 Front Line Defenders. Digital Security Resources. https://www.frontlinedefenders.org/en/digital-security-resources (accessed Aug. 5, 2024).

22 UN Human Rights Council. (2021). Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises (UN Doc A/HRC/47/39/Add.2).

23 Eguren, E., & Caraj, M. (2009). Protection Manual for Human Rights Defenders. Protection International. https://www.protectioninternational.org/protection-manuals/2009-protection-manual-for-human-rights-defenders/ (accessed Aug. 5, 2024); Human Rights First. Resources for Human Rights Defenders. https://humanrightsfirst.org/wp-content/uploads/2022/10/HRF-Defenders-Resources.pdf (accessed Aug. 5, 2024); Protection International. (2014). Surveillance and Counter-Surveillance for Human Rights Defenders and Their Organisation. https://www.protectioninternational.org/wp-content/uploads/2022/12/Online-NO2_SURVEILLANCE-AND-COUNTER-SURVEILLANCE-FOR-HUMAN-RIGHTS-DEFENDERS-AND-THEIR-ORGANISATION-310315.pdf (accessed Aug. 5, 2024); Protection International. (2014). Human Rights Defenders at High Risk: Security Considerations for Their Families and Personal Lives. https://www.protectioninternational.org/wp-content/uploads/2022/12/Online-NO3_HRDS-AT-HIGH-RISK_SECURITY-CONSIDERATIONS-FOR-THEIR-FAMILIES-AND-PERSONAL-LIVES-310315.pdf (accessed Aug. 5, 2024); Front Line Defenders. (2007). Protection Handbook for Human Rights Defenders. https://tinyurl.com/bp9t2zs8 (accessed Aug. 5, 2024).

and digital security risks which leaves HRDs without adequate digital protection. These show the need for an evolving approach to the digital safety of HRDs and the role played by tool developers in developing digital security tools that involves the needs and lived realities of HRDs.

One of the ways of addressing this challenge is by ensuring that HRDs and tool developers continuously engage with each other.[24] According to eyeWitness, such collaboration that makes public interest technology safer for HRDs can be achieved through setting up working groups and partnerships between HRDs, tool developers and academics to evaluate the security of tools.[25] Additionally, while citing good and bad examples of why human rights technology must be free and open-source, HURIDOCS noted the importance of building digital security tools with HRDs and not as experts for them.[26] However, as it concerns this research, there are limited resources in African contexts on how to ensure continuous engagements between HRDs who need digital security tools for effective protection and tool developers who design these tools.

THERE ARE LIMITED RESOURCES IN AFRICAN CONTEXTS ON HOW TO ENSURE CONTINUOUS ENGAGEMENTS BETWEEN HRDS AND TOOL DEVELOPERS.

Most resources focusing on the digital security of HRDs rarely provide any information on such engagement or how to achieve it in African contexts. Such continuous engagement could provide both actors with the context for developing the right tools while also ensuring iterative development of digital security tools that ensures active contributions from HRDs. This also provides an opportunity for HRDs from similar challenging contexts to exchange ideas and tool developers from diverse backgrounds to design interoperable tools to enhance digital security for HRDs in underserved and repressive political contexts. These will help address some of the challenges faced by HRDs which include low internet connectivity, lack of documentation skills, and limited digital security literacy.

24 The Engine Room. (2016). Technology Tools in Human Rights. https://www.theengineroom.org/wp-content/uploads/2016/12/technology-tools-in-human-rights.pdf (accessed Aug. 7, 2024).

25 Betts, W., & Llorente, R. V. (July 17, 2020). Making Public Interest Technology Safer for Human Rights Defenders. eyeWitness to Atrocities. https://www.eyewitness.global/Making-public-interest-technology-safer-for-human-rights-defenders.html (accessed Sept. 9, 2024).

26 Antin, K. (March 6, 2017). Why Secure Human Rights Technology Must Be Free and Open Source. HURIDOCS. https://huridocs.org/2017/03/why-secure-human-rights-technology-must-be-free-and-open-source/ (accessed Sept. 9, 2024).

This is where this report comes in, to understand the digital security landscape for HRDs in specific African contexts, their use of digital security tools, what tool developers can do better and how. Digital security tools are no longer a nice-to-have for HRDs and at the same time, these tools should be developed with the needs of HRDs in mind. This is primarily because in the digital age, digital security risks such as unauthorised access to personal information and communication could lead to physical violence or even death.[27] To combat such unauthorised access, HRDs must be able to provide tool developers with their experiences as HRDs and as digital security tool consumers.

Given this regional background, this report investigates the use of digital security tools by HRDs through survey responses and interviews. It also engages tool developers through surveys and interviews to understand how they receive and implement feedback from these HRDs to find how the information provided can be used to build and improve these digital security tools. These case studies do not necessarily represent the entire African context primarily because of the sample size and geographic scope.

DIGITAL SECURITY TOOLS SHOULD BE DEVELOPED WITH THE NEEDS OF HRDs IN MIND.

27 See Unwanted Witness (n 18).

4. Country studies: Democratic Republic of the Congo, Kenya, Senegal and Zimbabwe

The survey was conducted between October 2024 and February 2025 and gathered responses from 41 HRDs across four African countries: the Democratic Republic of the Congo (11), Kenya (10), Senegal (10), and Zimbabwe (10). All the HRDs work on various human rights themes with more than 60% focusing on civil and political rights while others focused on socio-economic rights and environmental rights. More than half of the respondents were women, offering valuable gendered insights into digital security practices and challenges. The survey aimed to understand how HRDs use digital security tools and the barriers they face. It explored themes such as political and legal environments, access to digital infrastructure, digital security skills and tool usage, digital security needs of HRDs and tool developers' perspectives.

MORE THAN 60% OF THE HRDs SURVEYED FOCUS ON CIVIL AND POLITICAL RIGHTS WHILE OTHERS FOCUS ON SOCIO-ECONOMIC RIGHTS AND ENVIRONMENTAL RIGHTS.

4.1 Political environment and surveillance

The political environment in which HRDs operate across the case studies plays a critical role in shaping their digital security practices. As noted by 85% of the HRDs, they face varying degrees of state surveillance, censorship, and legal repression, all of which significantly impact their ability to work safely and effectively. Across the four countries, the real and perceived fear of surveillance is widespread. A significant majority of HRDs are sure that they are being surveilled by state actors, with 65% of survey respondents expressing this concern. This also includes those with intermediate or advanced digital skills who report feeling targeted which points to the psychological toll of operating under constant threat from state actors.

DEMOCRATIC REPUBLIC OF THE CONGO

In the Democratic Republic of the Congo (DRC), over 90% of HRDs described the political climate as hostile toward civil society. One respondent shared, "*Sometimes it is difficult to make reports for fear of kidnapping.*"[28] Between 2020 and 2024, the country experienced violent unrest and increased electronic surveillance. In addition, HRDs are often labelled as collaborators or rebels, exposing them to abduction, intimidation, and digital monitoring by both civil and military intelligence agencies. "*The political environment is dominated by restrictions on fundamental freedoms*," one HRD explained, "*as is the case in a state of siege. Human rights defenders are not free to express themselves for fear of being labelled collaborators with rebels or Rwanda, the aggressor country in the DRC. We fear surveillance by the military authorities who rule the provinces of North Kivu and Ituri.*"[29]

"We fear surveillance by the military authorities who rule the provinces of North Kivu and Ituri."

This climate of fear also discourages HRDs from engaging openly online or using digital security tools that could expose them to further scrutiny. Several defenders reported targeted threats from government authorities. One HRD noted, "*This year, we've been working in a very hostile environment where the ruling power has become extremely repressive. Any activist who dares to criticise the government or speak out about community issues risks imprisonment or kidnapping.*"[30]

"Any activist who dares to criticise the government or speak out about community issues risks imprisonment or kidnapping."

Surveillance is a constant concern. "*Our environment is very hostile,*" said one HRD. "*Our phones and computers are monitored remotely, which puts us in danger because our data is often accessed by strangers.*"[31] Another HRD added, "*We are often listened to by the authorities, and our devices are regularly monitored.*"[32] According to transparency reports by one of DRC's

28 Human Rights Defender, DRC (Survey response, December 2024).

29 Human Rights Defender, DRC (Survey response, November 2024).

30 Human Rights Defender, DRC (Survey response, November 2024).

31 Human Rights Defender, DRC (Survey response, October 2024).

32 Human Rights Defender, DRC (Survey response, January 2025).

largest ISPs, Orange, in 2017, there were 981 customer data requests and 26 interception requests, and in 2022 there were 18 interception requests while customer data requests jumped to 1,228.[33] Orange also noted that out of the 26 countries it operates in, only two, Central African Republic and DRC, require continuous attention with respect to the protection of the rights to freedom of expression and privacy.

Goma, North Kivu, DRC (Ben Houdijk / Shutterstock.com)

KENYA

In Kenya, the digital security landscape for HRDs is deeply shaped by the country's political environment as noted by all the HRDs. As one HRD explained, "*Our work is heavily influenced by censorship, surveillance, and restrictive laws. Digital platforms often monitor and restrict activism-related content, limiting our reach and impact. The constant threat of surveillance makes secure communication difficult, as we are frequently targeted by both state and non-state actors.*"[34]

> *"The constant threat of surveillance makes secure communication difficult."*

All HRDs surveyed agreed that the political climate has become increasingly repressive since the 2022 administration came to power. They reported facing growing levels of censorship, targeted surveillance, and politically motivated audits. One HRD described the situation as "*very charged*," noting a rise in

33 CIPESA. (2019). State of Internet Freedom: Democratic Republic of the Congo. https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-the-Democratic-Republic-of-Congo-2019.pdf (accessed Aug. 8, 2024); Orange. (2022). Orange Transparency Report for Freedom of Expression, Information and Respect for Private Life. https://gallery.orange.com/element?id=410662 (accessed Aug. 8, 2024).

34 Human Rights Defender, Kenya (Survey response, October 2024).

arbitrary arrests, abductions, and even deaths of individuals critical of the government.[35] "*As a human rights defender*," one HRD said, "*I now have to be extremely cautious about what I post and how I share information online*."[36]

"I now have to be extremely cautious about what I post and how I share information online."

Government measures such as blocking platforms like Telegram and enforcing mandatory International Mobile Equipment Identity (IMEI) registration have negatively impacted internet freedoms.[37] These measures have created a chilling effect that discourages HRDs from using secure communication tools for fear of being surveilled. One HRD shared a personal account: "*I have been followed through my phone. It has been tapped several times, and I have had to replace it. My Facebook and Twitter accounts were also suspended while I've received threats through calls and messages*."[38] This presents an example of digital repression which not only limits the ability of HRDs to operate safely but also undermines their rights to expression, privacy, and association.

"My phone has been tapped several times, and I have had to replace it."

In 2021, Defenders Coalition noted the concerns of 56 HRDs in a report about their communications being intercepted.[39] Additionally, there are also concerns that state actors have access to call data and location information of HRDs.[40] In June 2024, Kenya witnessed nation-wide protests against a finance bill that was passed by state authorities. Marred by police brutality, enforced disappearances and abductions, many protesters, including HRDs noted that these violations were enabled by unlawful state-sanctioned

35 Human Rights Defender, Kenya (Survey response, November 2024).

36 Human Rights Defender, Kenya (Survey response, November 2024).

37 Wothaya, J. (Nov. 8, 2024). Telegram Access Blocked in Kenya. KICTANet. https://www.kictanet.or.ke/telegram-access-blocked-in-kenya/ (accessed June 30, 2025); Kenya Revenue Authority. (Nov. 5, 2024). Declaration of Mobile Devices Incorporating IMEI Numbers at Importation. https://www.kra.go.ke/news-center/public-notices/2150-declaration-of-mobile-devices-incorporating-imei-numbers-at-importation (accessed June 30, 2025).

38 Human Rights Defender, Kenya (Survey response, January 2025).

39 Defenders Coalition (n 12).

40 Wothaya (n 37).

surveillance.[41] Most victims of abductions and enforced disappearances noted that they kept receiving strange phone calls which were allegedly used to triangulate their locations before abduction and enforced disappearance.[42]

Nairobi, Kenya (Mwivanda Gloria / Shutterstock.com)

SENEGAL

"This left me completely paralysed."

Seventy percent of the HRDs in Senegal shared that they constantly face the threats of imprisonment and increased surveillance for expressing contrary opinions to that of state actors during protests and election periods. Online freedoms have declined, and this is connected to political tensions which has led to government-ordered internet shutdowns and media restrictions. "*The internet outage affected my work and disrupted the national economy. I could not communicate with my loved ones, trainees, or family and this left me completely paralysed.*"[43] Another HRD and journalist also shared that their work was negatively impacted during the politically charged years of 2021 and

41 Shabibi, N., Lauterbach, C., & Nation Team. (Oct. 29, 2024). Exclusive: How Kenyan Police Use Mobile Phones to Track, Capture Suspects. Daily Nation. https://nation.africa/kenya/news/exclusive-how-kenyan-police-use-mobile-phones-to-track-capture-suspects-4804416 (accessed June 30, 2025); ARTICLE 19. (June 28, 2024). Kenya: Guarantee Internet Access and Stop Surveillance of Protesters. https://www.article19.org/resources/kenya-guarantee-internet-access-and-stop-surveillance-of-protesters/ (accessed Aug. 8, 2024).

42 Business & Human Rights Resource Centre. (2024). Kenya: Safaricom Denies Claims of Supporting Surveillance of Perceived Leaders of Protests against High Taxation. https://www.business-humanrights.org/en/latest-news/kenya-safaricom-denies-claims-of-supporting-surveillance-of-perceived-leaders-protests-against-high-taxation/ (accessed Aug. 13, 2024); Business & Human Rights Resource Centre. (2024). Protests in Kenya: Alleged Breach of Privacy to Aid Surveillance, Denial of Access to Information and Consumer Boycott; Includes Safaricom's Comments. https://www.business-humanrights.org/en/latest-news/kenya-govt-urged-to-restore-internet-during-protests-as-concerns-about-surveillance-aided-by-telecoms/ (accessed Aug. 13, 2024).

43 Human Rights Defender, Senegal (Survey response, November 2024).

2024 whereby access to online information became difficult due to government-imposed internet shutdowns.

HRDs also noted a rise in state-sanctioned repression under the previous administration in Senegal. "*Restrictions on freedom of expression and internet shutdowns have undermined our advocacy and awareness-raising efforts*," one defender explained. "*Voicing opinions that differ from those of political leaders can be dangerous and may lead to imprisonment*."[44] The legal environment remains vague, allowing authorities broad discretion to suppress online expression. Disinformation campaigns further complicate the digital space, eroding trust in platforms and increasing the vulnerability of HRDs to state surveillance.

"It has undermined our advocacy and awareness-raising efforts."

In 2018, the government passed a vaguely worded electronic communications bill into law that had provisions that expanded the surveillance powers of state agents.[45] In 2021, the penal and criminal procedure codes were also amended to increase the surveillance powers of law enforcement agencies.[46] There are also reports noting that state actors are actively involved in monitoring citizens' communications.[47]

Dakar, Senegal (Pierre Laborde / Shutterstock.com)

44 Human Rights Defender, Senegal (Survey response, October 2024).

45 Freedom House. (2023). Freedom in the World: Senegal. https://freedomhouse.org/country/senegal/freedom-world/2023 (accessed Aug. 13, 2024).

46 Freedom House (n 45).

47 CIPESA (n 4); CIPESA. (Sept. 30, 2021). How State Surveillance Is Stifling Democratic Participation in Africa: State of Internet Freedom in Africa Study Findings. https://cipesa.org/2021/09/how-state-surveillance-is-stifling-democratic-participation-in-africa-state-of-internet-freedom-in-africa-study-findings/ (accessed Aug. 13, 2024); Institute of Development Studies. (Oct. 21, 2021). State Surveillance of Citizens Going Unchecked across Africa. https://www.ids.ac.uk/news/state-surveillance-of-citizens-going-unchecked-across-africa/ (accessed June 30, 2025).

ZIMBABWE

"Repressive laws further shrink civic space by restricting civil society operations and funding."

All the HRDs surveyed in Zimbabwe also describe the political and legal environment as marked by authoritarian control and systemic repression. "*Zimbabwe's unsafe political climate makes it dangerous for HRDs like me to engage in social justice work without being labelled enemies of the state, and this has led to fear of abductions, growing self-censorship, and the use of lawfare to silence those who disagree with government actions or policies.*"[48] Some of the laws used in lawfare tactics by state actors include the Cyber and Data Protection Act, 2021 and the Patriotic Law, 2023 which have been used to criminalise dissent and limit internet freedoms in Zimbabwe. Another HRD explained, "*The political environment in Zimbabwe significantly affects our human rights work as it is characterised by repression, surveillance, and restrictions of fundamental freedoms. Repressive laws, such as the Private Voluntary Organisation Bill, further shrink civic space by restricting civil society operations and funding.*"[49]

Supported by overbroad laws, state-sanctioned unlawful surveillance is equally rife in Zimbabwe.[50] This surveillance, which also includes unlawful surveillance of HRDs, has caused chilling effects in the country. In many instances, HRDs have had to resort to self-censorship while surveillance in Zimbabwe is characterised by state-non-state actor collaboration and platform infiltration and monitoring.[51] Some of the violations faced by HRDs include arbitrary arrests, surveillance, and pressure to self-censor particularly when they are working on politically sensitive issues. State actors also impose internet shutdowns during political events such as protests or elections which isolates HRDs and limits their ability to communicate safely online.

Additionally, HRDs fear that the government's access to citizens' data through mandatory SIM card registration, collection of biometrics and use of surveillance technologies such as CCTV cameras pose huge risks to their physical and digital safety.[52] This concern has increased as Zimbabwe is now described as a surveillance state, and at least, two reasons

48 Human Rights Defender, Zimbabwe (Survey response, October 2024).

49 Human Rights Defender, Zimbabwe (Interview, October 2024).

50 Murray & others (n 10); MISA Zimbabwe. Surveillance and Privacy. https://zimbabwe.misa.org/issues-we-address/surveillance-and-privacy/ (accessed Aug. 15, 2024).

51 Murray & others (n 10).

52 Matiashe, F. S. (Feb. 14, 2024). Zimbabwe: Digital Rights Activists Fear Misuse of Surveillance Cameras in Bulawayo. The Africa Report. https://www.theafricareport.com/336723/zimbabwe-digital-rights-activists-fear-misuse-of-surveillance-cameras-in-bulawayo/ (accessed Aug. 15, 2024).

have been adduced for this. One, the state's relationship with the Chinese government and its businesses in the purchase and use of surveillance spywares and tools.[53] Two, the military-driven investments in surveillance tools.[54] Reports have noted that HRDs face dangerous security risks as a result of state-sanctioned surveillance.[55]

As shown above, HRDs face an adverse operational environment to effectively carry out their work. This clearly reveals the multi-dimensional risks faced by HRDs in adopting digital security tools.

Harare, Zimbabwe (Noah Denhe / Pexels.com)

4.2 Access to digital infrastructure

According to 80% of the surveyed HRDs, access to digital infrastructure such as affordable internet, devices and human rights technologies remain a major challenge for HRDs across the four case studies. In spite of the differing levels of technological infrastructure and development, HRDs in all contexts face constant challenges that hinder their ability to effectively adopt and use digital security tools.

53 Global Voices. (Jan. 10, 2023). How Zimbabwe Is Building a Big Brother Surveillance State. https://advox.globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/ (accessed Aug. 15, 2024).

54 Munoriyarwa, A. (2022). The Militarization of Digital Surveillance in Post-Coup Zimbabwe: "Just Don't Tell Them What We Do". Security Dialogue, 53(5), 456–474. https://doi.org/10.1177/09670106221118796 (accessed June 30, 2025).

55 Southern Africa Human Rights Defenders Network. (2021). Zimbabwe Human Rights Defenders Assets and Needs Assessment. https://africandefenders.org/wp-content/uploads/2021/04/Zimbabwe-Human-Rights-Defenders-Assets-and-Needs-Assessment-Final.pdf (accessed Aug. 15, 2024); DefendDefenders. (Jan. 30, 2019). Zimbabwe: End Crackdown on Freedom of Assembly and Expression, and Harassment of Human Rights Defenders. https://defenddefenders.org/zimbabwe-end-crackdown-on-freedom-of-assembly-and-expression-and-harassment-of-human-rights-defenders/ (accessed Aug. 15, 2024).

DEMOCRATIC REPUBLIC OF THE CONGO

As one of the HRD from the DRC observed, "*We are already working in difficult conditions. Internet accessibility and connectivity remain extremely limited in rural and conflict-affected areas, and many activists are unfamiliar with digital security tools.*"[56] This statement shows a broader reality in the DRC, where internet access is highly uneven and largely concentrated in urban centres. Internet connectivity is often unreliable or unavailable in most remote and conflict-prone regions.

80% OF THOSE SURVEYED SHARED THAT ACCESS TO DIGITAL INFRASTRUCTURE REMAINS A MAJOR CHALLENGE.

The high cost of internet services and the unreliability of internet connections also complicate the HRDs' access to digital infrastructure. This complication also includes HRDs who are able to use digital security tools as they usually rely on low-cost devices and free applications which lack robust security features that are not suited for their contexts. Another HRD noted financial and technical barriers: "*Internet access is not at all affordable for the majority of activists. Secure devices and premium software like VPNs are completely inaccessible. Additionally, many HRDs in the DRC still lack the necessary digital skills.*"[57]

> *"Internet accessibility and connectivity remain extremely limited in rural and conflict-affected areas."*

A third HRD emphasised the challenges of operating in environments with limited digital infrastructure: "*It's very difficult to work. There are frequent network disruptions. I'm 90 kilometres from Kinshasa, where I have activities, but killings are happening on the Bateke Plateau and there's no way to make a call or send messages. We're trying to install the Signal app, but there's no network.*"[58]

56 Human Rights Defender, rural DRC (Survey response, October 2024).

57 Human Rights Defender, DRC (Survey response, February 2025).

58 Human Rights Defender, DRC (Interview, January 2025).

The International Telecommunications Union (ITU), as of 2023, reported that only 26.2% of the population use the internet in DRC while 48.6% own mobile phones.[59] In the annual report which rates countries based on how they protect freedoms by Freedom House for 2023, DRC was rated 'Not Free.'[60] Provisions of certain laws including the Telecommunications Act of 2002 give state actors unfettered access to personal communication of individuals through ISPs.[61]

"I'm 90 kilometres from Kinshasa. killings are happening on the Bateke Plateau and there's no way to make a call or send messages."

KENYA

Digital infrastructure is more advanced in Kenya, however, the cost of internet access remains a significant obstacle in rural counties according to all the HRDs surveyed. Furthermore, constant power outages also impact connectivity, and many HRDs use personal, low-specification devices that are not safe for running secure applications. An HRD observed that, "*Rural areas often lack reliable or affordable connectivity. Many HRDs in these regions rely on mobile data, which can be costly and limit extensive online activities… constant power outages in some areas is another challenge which further disrupts the effective use of technology.*"[62] The lack of awareness and access to human rights-focused technologies compounds these challenges. The HRD further explains that "*Awareness and use of digital security tools among HRDs vary significantly, with some familiar with encrypted apps like Signal, while others face barriers such as lack of training, limited resources, language challenges, low bandwidth, and outdated devices.*"

"Constant power outages in some areas is another challenge."

In terms of internet usage, 38.2% of the population use the internet in Kenya while 53.8% own mobile

59 International Telecommunications Union. (2023). Democratic Republic of Congo: ICT Development Index. DataHub. https://datahub.itu.int/dashboards/idi/?id=1&e=COD&y=2023 (accessed Aug. 8, 2024).

60 Freedom House. (2024). Freedom in the World: Democratic Republic of the Congo. https://freedomhouse.org/country/democratic-republic-congo/freedom-world/2024 (accessed Feb. 20, 2025).

61 FRANCE24. (June 10, 2019). Israeli "21st-Century Mercenaries" Spied for DR Congo's Kabila, Report Says. https://www.france24.com/en/20190610-israel-congo-kabila-black-cube-spying-uvda (accessed Aug. 8, 2024); Media Policy and Democracy Project. (2021). Digital Surveillance and Privacy in DRC: Balancing National Security and Personal Data Protection. http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/drc_report.pdf (accessed Aug. 8, 2024).

62 Human Rights Defender, rural Kenya (Survey response, October 2024).

phones.[63] In a recent report that rates countries according to how they protect internet freedom, Kenya was rated 'Partly Free.'[64] Civil society actors have also noted the state has infrastructure and mechanisms backed by overbroad legal provisions that allow backdoor access to personal communications to conduct widespread surveillance including those of HRDs.[65] While there are existing laws on communication surveillance in Kenya, civil society has noted that these laws further put HRDs at risk and provide no buffer against widespread use of surveillance tools by state actors against HRDs.[66]

SENEGAL

According to the ITU, in 2023, 55% of the Senegalese population use the internet while 76.5% own mobile phones.[67] In addition to this, government-imposed internet shutdowns during political events have further restricted internet access. One HRD explained, "*Exorbitant data costs and unreliable internet access in rural areas are a problem in Senegal. Over the past four years, due to a turbulent presidential election process, we have experienced internet shutdowns that have never occurred in the past. Since Senegal became connected to the internet in 1996, this is the first time we have experienced government-ordered internet shutdowns.*"[68]

"Over the past four years, due to a turbulent presidential election process, we have experienced internet shutdowns that have never occurred in the past."

63 International Telecommunications Union. (2023). Kenya: ICT Development Index. DataHub. https://datahub.itu.int/dashboards/idi/?id=1&e=KEN&y=2023 (accessed Aug. 8, 2024).

64 Freedom House. (2023). Internet Freedom Scores. https://freedomhouse.org/countries/freedom-net/scores (accessed Aug. 14, 2024).

65 American Friends Service Committee (n 1); Wanyonyi, P. (Feb. 19, 2017). Chilling Implications of State's Plan to Snoop on Your Phone Calls. The Standard. https://www.standardmedia.co.ke/counties/article/2001229908/chilling-implications-of-states-plan-to-snoop-on-your-phone-calls (accessed June 30, 2025); Privacy International. (March 23, 2021). Defenders Coalition: Impact of Communication Surveillance on HRDs in Kenya. http://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya (accessed Aug. 8, 2024).

66 Kapiyo, V., & Monyango, F. (2024). Surveillance Laws and Technologies Used in Countering Terrorism and Their Potential Impact on Civic Space. KICKTANet. https://www.kictanet.or.ke/?mdocs-file=49126 (accessed Aug. 8, 2024).

67 Ngugi, K., & Owino-Wamari, Y. (Aug. 30, 2018). Human Rights Defenders Securing the Right to Vote in Kenya. CIVICUS. https://www.civicus.org/index.php/re-imagining-democracy/stories-from-the-frontlines/3436-human-rights-defenders-securing-the-right-to-vote-in-kenya (accessed Aug. 13, 2024).

68 Human Rights Defender, rural Senegal (Survey response, February 2025).

Another HRD and journalist shared, "*As a Senegalese journalist and human rights defender, I have had to work in a context where access to the internet and technology has been hampered by constant outages during periods of political tension, such as those in 2021 and 2022. These outages, along with the closure of certain media outlets, such as Walf TV, have affected our ability to freely inform. Although internet access is widespread, costs remain high and access is limited in some regions, hampering the exercise of freedom of expression.*"[69] Additionally, another HRD noted that language barriers also hinder the effective use of many digital security tools, especially those not localised for Francophone or indigenous language users.[70]

"Internet outages, along with the closure of certain media outlets, such as Walf TV, have affected our ability to freely inform."

ZIMBABWE

In Zimbabwe, all HRDs surveyed are faced with some of the most protracted infrastructural barriers to digital security. Not only is the cost of internet access and digital devices prohibitively high, internet connectivity is constantly disrupted by power outages and politically motivated internet shutdowns are on the increase. A Zimbabwean HRD shared that, "*High data costs, erratic power supply, government-imposed internet shutdowns, and unlawful surveillance threaten freedom of expression, access to information, and the safety of HRDs.*"[71] These difficulties are even more pronounced for WHRDs in rural areas who encounter additional socio-economic and gender-based hurdles. A WHRD noted, "*Women and young women in rural areas remain largely digitally excluded, as most of them cannot afford smartphones… Community activists and HRDs, who are mostly young women in rural and peri-urban communities, still face serious challenges in accessing the internet.*"[72] These faceted risks significantly limit

"Women and young women in rural areas remain largely digitally excluded."

69 Human Rights Defender, Senegal (Survey response, February 2025).

70 Human Rights Defender, Senegal (Survey response, January 2025).

71 Human Rights Defender, Zimbabwe (Interview, October 2024).

72 Woman Human Rights Defender, Zimbabwe (Survey response, October 2024).

the ability of HRDs, especially women in areas with low-bandwidth to engage safely and effectively in digital spaces.

In 2023, the ITU reported that 29.3% of the population in Zimbabwe use the internet while 47% of the population also own mobile phones. According to Freedom House, with respect to Global Freedom scores, Zimbabwe is rated "Not Free."[73]

Across all four countries, HRDs often rely on outdated personal devices that lack the technical capacity to support secure applications and this limits their ability to adopt tools that require higher processing power, regular updates, or stable connectivity. The financial burden of upgrading or replacing devices is also a major obstacle for grassroots defenders who operate in under-resourced settings.

Power instability is also a recurring issue, especially in rural Kenya and Zimbabwe, where constant outages disrupt digital communication and limit the use of digital security tools that require consistent power and internet access. These pre-existing and fundamental infrastructural gaps are worsened by conflict in the DRC that often leads to targeted internet disruptions and pervasive surveillance.

As shown above, the challenges faced by HRDs have a direct impact on their digital security practices. The tools that require high bandwidth, regular updates, or constant internet access are often not fit-for-purpose especially for HRDs who live in remote or conflict zones. As a result, many HRDs resort to platforms that are widely accessible but less secure which may compromise their digital safety. The challenges are worse for WHRDs including those who work in rural areas and face intersecting barriers including socio-economic constraints, limited digital literacy, and gender-related prejudice. These barriers significantly restrict their access to secure digital tools and training opportunities.

TOOLS THAT REQUIRE HIGH BANDWIDTH, REGULAR UPDATES, OR CONSTANT INTERNET ACCESS ARE OFTEN NOT FIT-FOR-PURPOSE ESPECIALLY FOR HRDs WHO LIVE IN REMOTE OR CONFLICT ZONES.

73 Freedom House. (2023). Global Freedom Scores. https://freedomhouse.org/countries/freedom-world/scores (accessed Aug. 14, 2024).

4.3 Digital security skills and tool usage

The digital security landscape for HRDs in African contexts is shaped not only by access and political context but also by the level of digital security skills, the types of tools available and in use. The findings from the survey in the four country case studies show varying skill levels, different preferences for digital security tools, and usability challenges that influence how HRDs engage with digital security technologies.

VARYING SKILL LEVELS, DIFFERENT PREFERENCES, AND USABILITY CHALLENGES INFLUENCE HOW HRDs ENGAGE WITH DIGITAL SECURITY TECHNOLOGIES.

DIGITAL SECURITY SKILLS

HRDs report different levels of digital security skills across the four countries. For example, 40% of HRDs surveyed identified that they have basic skills, while 40% noted that they have intermediate skills with only 20% sharing their skills as advanced. This shows that a major number of HRDs have some familiarity with digital security tools while a majority still operate without the advanced skills required to leverage secure technologies or respond effectively to digital threats in high-risk political environments.

TOOL USAGE

Digital tools commonly used by HRDs are as a result of necessity and accessibility. For example, email remains universal (used by 100% of respondents) which is followed by social media platforms such as Facebook, Instagram, and WhatsApp (85%). HRDs use these tools for communication, advocacy, and organising, regardless of their known security limitations. Some of these digital security tools include Signal (50%) and VPNs (40%) which are valued for their privacy-enhancing features and ability to bypass censorship. Other tools mentioned by HRDs in the survey include encrypted email services (e.g., ProtonMail), password managers (e.g., KeePass, Bitwarden), and anti-censorship tools like TAILS and Tor VPN.

USABILITY

> *"Signal is not popular. you have to use WhatsApp, which is not safe for HRDs."*

In spite of the availability of digital security tools, usability remains a major challenge for many HRDs. Many HRDs report that these tools are often too technical or difficult to use which require multiple steps for setup. A woman HRD from Zimbabwe shared, "*When we have provided feedback or sought help, the technical complexity of the tools sometimes posed challenges for our team, who often lack the technical expertise to communicate needs in a way that developers could easily address*." This is difficult for those with only basic digital literacy or limited access to training. An HRD from Senegal noted, "*Tools like Signal are difficult to use to communicate with people. For example, very few people are using the Signal app in Senegal. Signal is not popular. So, if you want to communicate with people, you have to use WhatsApp, which is not safe for HRDs.*"[74]

PEER ADOPTION

The point above leads to another important factor: peer adoption. Digital security tools are only effective when parties in a conversation use them and are widespread among HRD communities who need them. HRDs struggle to communicate securely in environments where digital security tools are not adopted by peers and as a result, they are often forced to revert to less secure platforms to maintain communication with colleagues, partners, or communities.

TRAINING

The effectiveness of digital security tools is closely tied to previous and continuous training. This is because those who have received detailed digital security training before are more likely to report positive experiences with tools such as Signal, TAILS, and VeraCrypt. One of the HRDs noted that "*I use Signal a lot for secure messaging and calling, utilising its disappearing messages feature for enhanced security*."[75] These tools are praised for their ease of use and built-in security features when users understand how to navigate them. On the other hand, those without training often struggle with tool adoption which often leads to inconsistent and insecure practices.

74 Human Rights Defender, Senegal (Survey response, February 2025).

75 Human Rights Defender, DRC (Survey response, February 2025).

"The challenge is for women HRDs operating at community level especially in rural areas they have no access to reliable, affordable and consistent internet and suitable gadgets."

The findings also showed the gendered dimension of digital security skills. This is because WHRDs in rural areas confront additional barriers to acquiring digital security skills due to limited access to training, lower digital literacy, and socio-cultural constraints. One of the WHRDs from Zimbabwe noted that, "*As a civil society leader I do have access to internet and devices but the challenge is for women HRDs operating at community level especially in rural areas they have no access to reliable, affordable and consistent internet and suitable gadgets.*" These disparities demonstrate the need for gender-sensitive training programmes and tools designed with inclusivity in mind. Another WHRD from Kenya noted that, "*While these tools are a step in the right direction, they are not fully optimised to meet the complexities of our environment. More context-specific, affordable, and user-friendly solutions, alongside capacity-building efforts, would better address our needs.*"

"These tools are not fully optimised to meet the complexities of our environment."

Marsabit town, Kenya (Matyas Rehak / Shutterstock.com)

5. Digital security needs of HRDs

A CENTRAL THEME EMERGING FROM ALL THE SURVEY RESPONSES IS THE CRITICAL NEED FOR TRAINING AND CAPACITY BUILDING.

The challenges faced by HRDs identified above, at least in the DRC, Kenya, Senegal and Zimbabwe, have laws that limit encryption, compel assistance from service providers to provide personal information and make SIM card registrations mandatory.[76] This demonstrates strong government access to personal information of subscribers including HRDs. It also explains why HRDs have expressed a clear and urgent need to strengthen their digital security. These needs reflect the realities of working in high-risk, under-resourced environments and show the importance of tools and training that are not only technically robust but also contextually relevant, accessible, and inclusive.

A central theme emerging from all the survey responses is the critical need for training and capacity building. An HRD noted that, "*Many human rights defenders lack the training or resources to fully understand or implement digital security tools.*"[77] HRDs consistently emphasised that digital security knowledge must be widespread, practical, and tailored to varying levels of digital literacy. As one respondent put it, "*Basic levels of digital literacy and security skills create barriers to effectively utilising the tools for maximum protection. Lack of access to regular training opportunities exacerbates this issue.*"[78] Training should cover a spectrum of skills from basic practices like password management and two-factor authentication to more advanced topics such as threat modelling, secure communication, and data encryption. Such training should also cover different types of digital security tools that includes both technical and non-technical tools.

76 CIPESA. (2021). How African Governments Undermine the Use of Encryption. https://cipesa.org/wp-content/files/briefs/How_Africa_Government_Undermine_the_Use_of_Encryption_2021.pdf (accessed June 30, 2025.

77 Human Rights Defender, Zimbabwe (Survey response, January 2025).

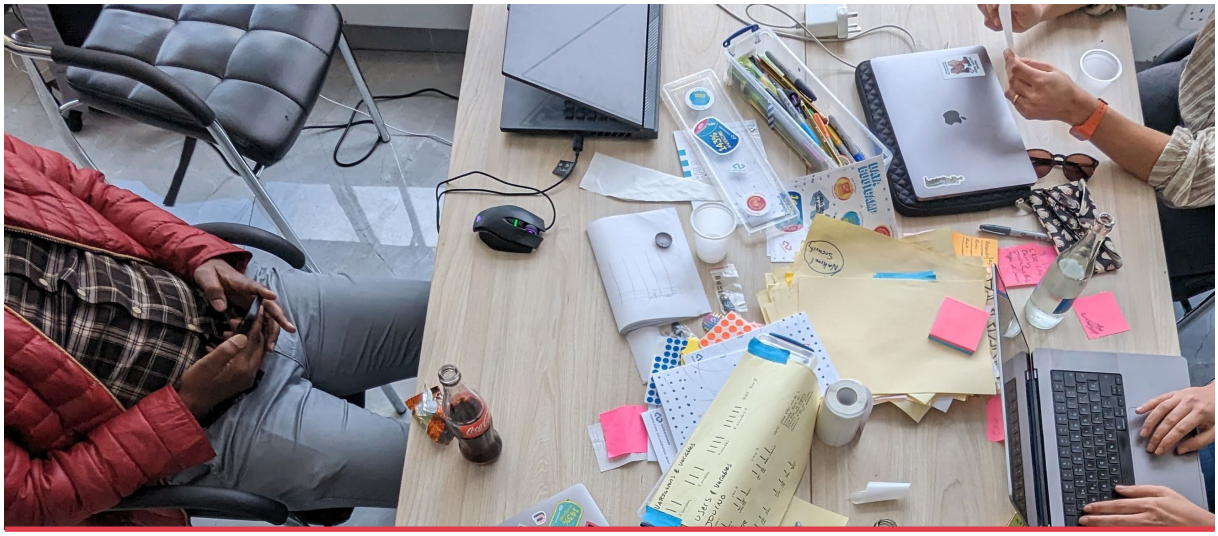
78 Human Rights Defender, Kenya (Interview, November 2024).

"Training should cover basic to advanced security practices, threat identification, and how to handle digital attacks."

A WHRD from Zimbabwe shared the following about their needs: "*Receiving regular, accessible training programmes on how to use digital security tools effectively. This should cover basic to advanced security practices, threat identification, and how to handle digital attacks. Training should be available in local languages and tailored to the literacy levels of the target audience.*" Importantly, HRDs called for training that is regular, hands-on, and community-based. Many expressed a desire for mentorship programmes and peer learning opportunities that would allow them to build confidence and independence in using digital security tools. NGO spaces, they suggested, should be capacitated to serve as hubs for digital security education and support.

Furthermore, HRDs identified that digital security tools must be affordable and adapted to their specific contexts. As a result, most HRDs' needs are focused on improving the design and usability of digital security tools. Many tools currently in use are perceived as too technical or not suited for environments with low bandwidth, infrequent power supply, or limited internet access.

MANY TOOLS ARE PERCEIVED AS NOT SUITED FOR ENVIRONMENTS WITH LOW BANDWIDTH, INFREQUENT POWER SUPPLY, OR LIMITED INTERNET ACCESS.



Nairobi, Kenya (Data4Change)

Major digital security needs of human rights defenders

EASE OF USE

HRDs seek out tools that have simple and easily accessible user interfaces that require minimal technical skills.

AFFORDABILITY AND ACCESSIBILITY

They also noted the need for tools that have free and low-cost features particularly for HRDs who work in rural or conflict settings.

OFFLINE FUNCTIONALITY

Digital security tools should also be capable of operating without constant internet access and have low-bandwidth access.

LOCALISATION

These tools should be made available in local languages for use and for providing feedback to facilitate usability across diverse linguistic communities.

SECURITY AND ANONYMITY

Tools must also include strong encryption, secure communication channels, and anonymity features for HRDs working in high-risk political environments and underserved contexts.

HRDs equally noted the importance of continuous support and maintenance for digital security tools. To them, these tools must be regularly updated to be able to respond to evolving threats, and users need access to troubleshooting assistance and rapid response protocols in the event of threats and attacks on their digital and physical safety. An HRD noted that "*It is very important to provide ongoing training and support*

"Provide ongoing training and support that involves HRDs in the development process."

that involves HRDs in the development process of digital security tools. This will ensure that these tools are practical, relevant, and responsive to our needs on the ground."[79] HRDs also made requests for secure data storage, backup solutions, and media monitoring tools.

"We would be keen to work with digital security tool developers to co-develop tools that address specific needs."

All the HRDs shared a strong interest in co-design and collaboration with digital security tool developers. One of the HRDs shared that, "*We would be keen to work with digital security tool developers to co-develop tools that address specific needs that we face based on different aspects of our socio-political, legal and economic context.*"[80] HRDs want to be involved in the creation and update of tools to ensure that their lived experiences and needs are reflected in the final products. This participatory approach is seen as essential to building trust, relevance, and long-term sustainability of digital security tools in African contexts.

The digital security needs of HRDs point to a comprehensive vision of digital security, one that goes beyond tools development or deployment to cover training and support. In order to meet these needs, there is an urgent need for coordinated efforts among developers, civil society, funders, and policymakers to ensure that HRDs are not only protected but also capacitated to face the cross-cutting risks challenges in their various contexts.

79 Human Rights Defender, DRC (Interview, February 2025).

80 Human Rights Defender, Kenya (Interview, December 2025).

6. Tool developers' perspectives

The survey gathered responses from developers of 11 digital security tools between February and March 2025, offering insights into the types of digital security tools being developed for HRDs, as well as the developers' approaches to localisation, user engagement, and feedback integration.

The digital security tools surveyed include a mix of well-established and emerging platforms such as Awala, Butter Box, Lethro, Mobile Surveillance Monitor (MSM), Shira, SMSWithoutBorders (RelaySMS and DekuSMS), TAILS, Tella, Tor VPN, and Uwazi.

DIGITAL SECURITY TOOL	DESCRIPTION
Awala	Awala is a network for data exchange with or without the internet.
DekuSMS	DekuSMS enables Android users to communicate using end-to-end encryption for SMS messaging. It works as a default SMS app with features that power RelaySMS (such as message forwarding).
Butter Box	Butter Box broadcasts its own Wi-Fi network, allowing users to install apps, join chat rooms, and communicate without an internet connection.
RelaySMS	RelaySMS allows users to communicate with digital platforms using encrypted SMS messaging while leveraging Signal's Double Ratchet algorithm.
Letro	Letro is a messaging app built on Awala, designed for use in internet shutdowns or conflict zones.
Mobile Surveillance Monitor (MSM)	MSM is a threat intelligence tool for analysing global surveillance threats targeting mobile users, offering forensic and network analysis capabilities.
Tella	Tella encrypts and hides files on mobile devices for secure documentation, and offers certain offline capabilities.
Shira	Shira trains users to detect and counter phishing attacks.
TAILS	TAILS is a portable operating system for privacy and censorship resistance.
Tor VPN	Tor VPN is an Android application that routes internet traffic through the Tor network to bypass censorship and surveillance while maintaining anonymity online.
Uwazi	Uwazi is a secure database tool for documenting human rights information and can be used alongside other digital security tools.

These tools serve a range of functions, from secure messaging and encrypted data storage to mobile surveillance monitoring and offline documentation. For example, SMSWithoutBorders allows for multiple phone numbers in case a previous number has been blocked while Butter Box and Awala allows for offline use. Their diversity reflects the broad spectrum of digital threats HRDs face and the need for tailored solutions across different operational contexts.

A key area of focus in the survey was language support and localisation. Developers reported varying levels of localisation capacity: some tools currently support multiple languages like Uwazi, others are browser-dependent such as MSM, and a few, such as SMSWithoutBorders, have no language support in place but plan to implement it. Notably, all developers, regardless of their current localisation status, expressed a strong interest in expanding language support and engaging more deeply with users to inform these efforts.

This openness to localisation is significant given the challenges HRDs face when using tools that are not available in local languages. Developers acknowledged that translation efforts must go beyond interface text to include user documentation, training materials, and support resources. This broader approach to localisation is essential for ensuring that tools are not only technically accessible but also culturally and linguistically relevant.

The survey responses also revealed that developers are increasingly aware of the importance of user-centred design. Many expressed interests in co-design workshops and periodic engagements with HRDs, recognising that direct collaboration can lead to more practical, context-aware tools. This interest is not merely aspirational as 90% of developers surveyed indicated a willingness to participate in ongoing co-design processes.

The developer profiles reflect a growing commitment to building tools that are secure, adaptable, and responsive to the lived realities of HRDs in Africa. While gaps remain in localisation and user engagement, there is a clear willingness among developers to bridge these divides through collaboration and feedback integration.

THE DEVELOPER PROFILES REFLECT A GROWING COMMITMENT TO BUILDING TOOLS THAT ARE SECURE, ADAPTABLE, AND RESPONSIVE TO THE LIVED REALITIES OF HRDs IN AFRICA.

6.1 Feedback mechanisms and responsiveness

All the tool developers surveyed demonstrated a growing recognition of the importance of user feedback in shaping the design, functionality, and relevance of digital security tools for HRDs. While most HRDs reported having little to no direct experience working with developers (60%), developers themselves indicated a strong commitment to improving feedback channels and responsiveness.

The survey responses from developers revealed that they all receive user-feedback using a variety of channels, including GitHub issue trackers, email, social media, partner organisations, and dedicated feedback portals. For example, SMSWithoutBorders accepts feedback using GitHub and emails while Awala, Lethro and MSM accept feedback from social media, emails and a submission portal. These multiple entry points are intended to make it easier for users to report bugs, suggest features, or raise usability concerns. However, the effectiveness of these channels depends on users' digital literacy, language proficiency, and awareness of how to engage with developers which are factors that remain uneven across HRD communities.

In terms of responsiveness, 70% of developers reported they respond to user-feedback while 20% shared that they are unable to address feedback due to limited funding. Ten percent do not see user-feedback as a priority and most of the developers reported that they prioritise feedback based on urgency, frequency, and feasibility. Issues that affect core functionality or user safety are typically addressed first, while feature requests or interface improvements may be scheduled for future updates. The open-source nature of many tools allows for more agile and community-driven development, enabling faster integration of user feedback when resources permit.

70% OF DEVELOPERS REPORTED THEY RESPOND TO USER-FEEDBACK WHILE 20% SHARED THAT THEY ARE UNABLE TO ADDRESS FEEDBACK DUE TO LIMITED FUNDING.

However, the extent to which feedback is integrated varies. Some tools are highly configurable and regularly updated, while others such as Tella, Shira, Awala, Lethro and MSM face constraints due to technical complexity, limited funding, or small development teams. Developers acknowledged these limitations but emphasised their willingness to improve through periodic user engagement and co-design processes. Encouragingly,

90% of developers expressed interest in ongoing collaboration with HRDs, including through co-design workshops and community-of-practice models. This reflects a shift toward more participatory development practices, where users are not only testers but also co-creators of the tools they use for their safety.

There are existing gaps in the accessibility and visibility of feedback mechanisms and developers are increasingly committed to building responsive, user-informed tools. It is important to strengthen these feedback loops through better communication, localisation, and structured engagement. These will be essential to ensuring that digital security tools evolve in step with the needs and realities of HRDs in African contexts.

6.2 Interest in collaboration

The majority of developers (90%) expressed openness to ongoing collaboration, including participation in co-design workshops, community-of-practice models, and periodic user engagement sessions. This willingness is not limited by the current capabilities of the tools; even developers whose tools lack full localisation or advanced features indicated a desire to work more closely with HRDs to improve usability and contextual relevance.

This collaborative spirit is echoed by HRDs themselves. According to the presentation, 85% of HRDs expressed strong interest in engaging with developers through structured, recurring formats. They emphasised that co-design is not just a technical process but a trust-building exercise that ensures tools are aligned with their operational realities such as low bandwidth, political repression, and limited digital literacy.

In spite of this shared enthusiasm, several barriers to deeper collaboration persist.

90% OF TOOL DEVELOPERS EXPRESSED OPENNESS TO ONGOING COLLABORATION.

85% OF HRDs EXPRESSED STRONG INTEREST IN ENGAGING WITH DEVELOPERS THROUGH STRUCTURED, RECURRING FORMATS

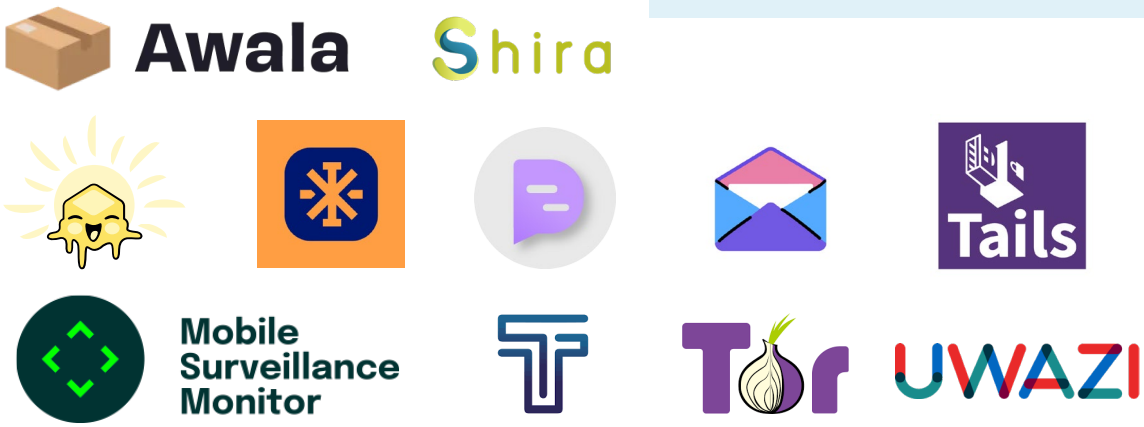
These include:

- Limited direct contact between HRDs and developers, with 60% of HRDs reporting no prior engagement.
- Resource constraints on both sides, including time, funding, and staffing, which limit the ability to sustain long-term collaboration.
- Lack of structured platforms or intermediaries to facilitate regular dialogue and feedback exchange.
- Language and cultural gaps which can hinder mutual understanding and the localisation of tools.

To address these challenges, both HRDs and developers have called for the creation of multi-stakeholder convenings and co-design frameworks that bring together users, developers, funders, and civil society actors. These platforms would enable iterative feedback, shared learning, and the co-creation of tools that are not only technically sound but also socially and politically grounded.

In summary, the survey shows a promising foundation for collaboration between HRDs and developers. While structural and logistical barriers remain, the strong mutual interest in co-design and engagement offers a clear path forward. Realising this potential will require investment in facilitation, translation, and long-term relationship-building to ensure that digital security tools are truly fit for purpose in the African human rights context.

THE STRONG MUTUAL INTEREST IN CO-DESIGN AND ENGAGEMENT OFFERS A CLEAR PATH FORWARD.



7. Bridging the gap between HRDs and tool developers in African contexts

The dual survey approach targeting both HRDs and tool developers offers a valuable, multi-perspective understanding of the digital security tools landscape in African contexts. While each survey provides rich insights into the experiences, needs, and practices of its respective group, the analysis reveals both limitations of the sample size and the gaps that must be addressed to foster more effective digital security ecosystems.

THE ANALYSIS REVEALS BOTH LIMITATIONS OF THE SAMPLE SIZE AND THE GAPS THAT MUST BE ADDRESSED TO FOSTER MORE EFFECTIVE DIGITAL SECURITY ECOSYSTEMS.

The HRD survey from defenders captures the lived experiences of individuals operating in politically repressive and technologically constrained environments. While the sample size of 41 respondents across the case studies are limited, the survey's strength lies in its ability to surface context-specific challenges such as unreliable internet, high costs, and surveillance threats while also noting common regional patterns, including reliance on platforms like WhatsApp and widespread fear of state surveillance.

However, the survey also reveals a disconnect between tool availability and usability. While HRDs are aware of tools like Signal, Tor, and TAILS, many lack the training or infrastructure to use them effectively. The data shows that 40% of HRDs have only basic digital security skills, and even those with intermediate knowledge often feel unprepared to navigate complex tools. This shows the need for localised, user-friendly, and low-bandwidth solutions, as well as ongoing training and mentorship. The HRD survey also demonstrates its gender representation as over half of respondents were women which allows for a more nuanced understanding of how gender intersects with digital insecurity.

The report reveals a strong willingness to collaborate with HRDs as 90% of developers expressed interest in co-design and periodic engagement. Tools such as Tella, Shira, Uwazi, and Butter Box reflect a growing ecosystem of open-source and rights-focused technologies. This report also identified barriers to deeper collaboration between HRDs

and tool developers, including limited funding, technical constraints, and the absence of structured platforms for continuous engagement.

Localisation also remains a major challenge. While some tools support multiple languages or plan to expand, many still lack comprehensive translation of interfaces, documentation, and training materials. This limits accessibility for non-English-speaking HRDs and reinforces the need for co-design practices.

This report points to a disconnect between tool design and user realities, but also to a shared desire for change. HRDs want tools that are affordable and context-aware. Developers want to build tools that are useful, secure, and widely adopted. The missing link is structured and continuous collaboration. Both groups support the idea of co-design workshops, communities of practice, and multi-stakeholder convenings. These mechanisms could help overcome barriers such as language, technical complexity, and resource limitations. However, realising this vision will require investment in facilitation, translation, and long-term relationship-building.

THIS REPORT POINTS TO A DISCONNECT BETWEEN TOOL DESIGN AND USER REALITIES, BUT ALSO TO A SHARED DESIRE FOR CHANGE.

This report provides some of the realities faced by HRDs in the use of digital security tools in African contexts. It demonstrates the urgency of addressing political, infrastructural and usability challenges while also pointing to a path forward, grounded in collaboration and co-creation between HRDs and tool developers. To move from insight to impact, stakeholders must invest in bridging the gap between tool developers and HRDs, ensuring that digital security solutions are not only technically sound but also socially embedded and user-driven.

8. Recommendations for action

For tool developers

a. Prioritise user-centred design

- Develop tools that are low-bandwidth and compatible with devices used in high-risk and under-resourced environments.
- Co-create both technical and non-technical digital security tools for HRDs and update these tools continuously to reflect changes.
- Ensure offline functionality of digital security tools to support HRDs in areas with unreliable internet.

b. Localise tools for contextual relevance

- Translate interfaces, documentation, and training materials into more local African languages.
- Adapt tools to cultural and political contexts to improve usability and trust.

c. Establish continuous feedback loops

- Create accessible feedback channels (e.g., in-app forms, community forums, in-person meetings).
- Regularly update tools based on user input to prioritise safety and usability.

d. Engage in co-design with HRDs

- Co-facilitate a secure two-way feedback system of engagement between HRDs and tool developers in underserved and repressive African contexts
- Facilitate participatory design workshops with HRDs to ensure tools meet real-world needs.
- Build long-term relationships with HRD communities for iterative digital security tools development, deployment and updates.

For civil society organisations and digital security experts

a. Provide regular and hands-on training

- Offer tiered training programmes (basic, intermediate, advanced) tailored to different skill levels.
- Focus on practical skills like secure communication, threat modelling, and data protection.

b. Build peer learning networks

- Encourage mentorship and knowledge-sharing among HRDs.
- Create regional hubs or communities of practice for ongoing support.

c. Support women and rural HRDs

- Design gender-sensitive training and tools that address the unique challenges faced by women HRDs.
- Ensure outreach and support for HRDs in rural and conflict-affected areas.

For donors and funders

a. Invest in open-source and rights-focused tools.

- Provide long-term funding for the development, maintenance, and scaling of secure digital security tools.
- Prioritise projects that emphasise transparency, inclusivity, and sustainability.

b. Support localisation and infrastructure.

- Fund translation efforts and the development of tools that work in low-resource environments.
- Invest in digital infrastructure (e.g., community internet access points, safe device subsidies).

c. Facilitate multi-stakeholder collaboration.

- Sponsor co-design workshops, tool developer-HRD convenings, and regional digital security forums.
- Encourage cross-sector partnerships to bridge technical and contextual gaps.

For governments and policymakers

a. Carry out legal reform in line with international human rights standards

- Carry out legal reform in line with international human rights standards.
- Repeal or amend existing provisions without adequate surveillance safeguards.
- Enact and implement rights-respecting laws on HRDs' protection.
- Repeal or amend legislation that criminalises encryption or facilitates unlawful surveillance.

b. Ensure accountability for surveillance abuses

- Strengthen existing access to justice mechanisms such as judicial and non-judicial remedial mechanisms for victims of unlawful surveillance.
- Promote transparency in the use of surveillance tools including publishing periodic information on surveillance requests.
- Establish independent and multi-stakeholder oversight mechanisms for surveillance practices.
- Investigate and sanction misuse of surveillance technologies against HRDs.

c. Promote safe civic spaces

- Guarantee the safety of HRDs under the law and in practice, online and offline.
- Ensure continuous human rights training for state actors involved in the purchase and use of surveillance technologies.
- Support public education campaigns on surveillance and responsible technology use.

9. Future directions

Key direction 1

LONGITUDINAL STUDIES ON TOOL ADOPTION AND IMPACT

Conduct long-term studies of specific respondents continuously to assess the adoption, effectiveness, and impact of digital security tools among HRDs. This will provide insights into the sustainability of digital security practices and the evolving needs of HRDs.

Key direction 2

GENDERED EXPERIENCES OF DIGITAL INSECURITY

Investigate the specific digital security challenges faced by women HRDs in rural areas. Explore the intersection of gender, digital literacy, and socio-economic barriers to develop targeted interventions.

Key direction 3

MORE COMPARATIVE STUDIES ACROSS AFRICAN CONTEXTS

Conduct comparative research to understand the similarities and differences in digital security practices and challenges across various African contexts. This will help identify context-specific solutions and best practices.

Key direction 4

CO-DESIGN AND MULTI-STAKEHOLDER ENGAGEMENT MODELS

Explore successful models of co-design and multi-stakeholder engagement in the development of digital security tools and identify best practices and lessons learned to inform future collaborative efforts.

10. Conclusion

The report demonstrated how HRDs in the DRC, Kenya, Senegal and Zimbabwe use digital security tools and what tool developers can do better and how. The surveys and interviews conducted with HRDs and tool developers revealed challenges faced by HRDs' use of digital security tools in the four countries. Human rights defenders face intersecting barriers, including unreliable internet access, expensive internet access, and pervasive surveillance, which hinder their ability to effectively use digital security tools. Tool developers also identify limited direct contacts with HRDs, lack of funding and other hurdles in developing relevant tools for HRDs. In spite of these challenges, there is a strong desire among HRDs for training and co-design opportunities with developers. Tool developers also show a willingness to collaborate and improve their tools based on user feedback. Therefore, in order to address the digital security needs of HRDs, a comprehensive approach that goes beyond technological solutions is required. This approach involves reforms in hostile political environments such as addressing surveillance abuses faced by HRDs, investing in affordable and accessible digital infrastructure such as internet and safe devices, continuous training and digital skills development for HRDs as well as facilitating continuous collaboration between HRDs, developers, civil society, funders, and policymakers.

Co-design workshops, communities of practice, and multi-stakeholder convenings are essential mechanisms that can bridge the gap between HRDs and tool development. These collaborative efforts will ensure that digital security tools are not only technically sound but also socially embedded and user-driven. To move from insight to impact, stakeholders must commit to coordinated and collaborative efforts to improve the digital security of HRDs in African contexts. For example, developers should prioritise contextually relevant design and localisation, while civil society organisations should continuously facilitate digital security training and programmes. Funders must provide long-term support for open-source, rights-focused tools, and policymakers should uphold internet freedoms and protect HRDs from surveillance and repression. In conclusion, digital security tools can both empower or strip human rights defenders of their safety, however, by working together, key stakeholders can create a safer digital environment for HRDs to carry out their vital work.

Appendices

Survey questions

FOR HRDS

1. Country:
2. What area of human rights does your work focus on?
3. How would you describe the context you work in as a human rights defender in terms of your access to affordable Internet, devices and human rights technology?
4. How has your work as a human rights defender been affected by your political environment?
5. Which digital tools do you use for your work on a day-to-day basis?
6. How would you describe your digital security skills?
7. Do you believe you are under digital surveillance?
8. If yes, by whom and how so?
9. Which digital security tools do you use?
10. How would you describe your experience using these tools?
11. What informed your choice of these digital security tools?
12. Do these tools support your contexts and needs? E.g. political environment; access to affordable internet, devices and human rights technologies; access to digital and literacy skills; access to digital security skills; provision for local language(s)?
13. What challenges do you face in using these digital security tools?
14. Can you share your experience working with tool developers?
15. What factors contributed to a smooth collaboration, and what challenges did you encounter?
16. What key lessons did you take away from this experience?
17. How can tool developers and other human rights stakeholders better address your digital security needs as a human rights defender?
18. Are you interested in periodic engagements including a community of practice and co-designing workshops with tool developers on how they can build safer digital security tools and existing ones?
19. Any other information you would like to share?

FOR TOOL DEVELOPERS

1. Country
2. What is/are the name(s) of the digital security tool(s) you have developed?
3. Provide a short description of the tool(s).
4. Does/do your tool(s) allow user feedback?
5. How do you address user feedback?
6. To what extent can your tool(s), as currently designed, be updated to accommodate user feedback?
7. How does/do your tool(s) ensure backchanneling by users in low resource and highly repressive environments?
8. What do you consider as optimal user experience for your tool(s) especially in low resource and highly repressive environments?
9. How many local African languages does/do your tool(s) support?
10. Do you have emergency response communication systems embedded in your tool(s)?
11. Are you interested in periodic engagements including a community of practice and co-designing workshops with users on how to make your tools safer?

Acknowledgements

This report was compiled in 2025 with HURIDOCS as the host organisation and financial support provided by Open Technology Fund. I am deeply grateful to all the HRDs, local organisations and tool developers who generously contributed their time to complete the survey, commit to disseminating the report and share their insights during interviews. I would also like to extend my sincere thanks to my colleagues at HURIDOCS: Yolanda Booyzen, Danna Ingleton, Bono Olgado, Alejandra Kaiser, Anastasia Vladimiro, and many others for their encouragement and guidance throughout the fellowship. I am also thankful to Wei Fan and Ongere Churchill at Open Technology Fund for their support.

Tomiwa Ilori
July 2025