Justice by design: reimagining rights-based responses to cybercrime in Africa

by **Tina Power**

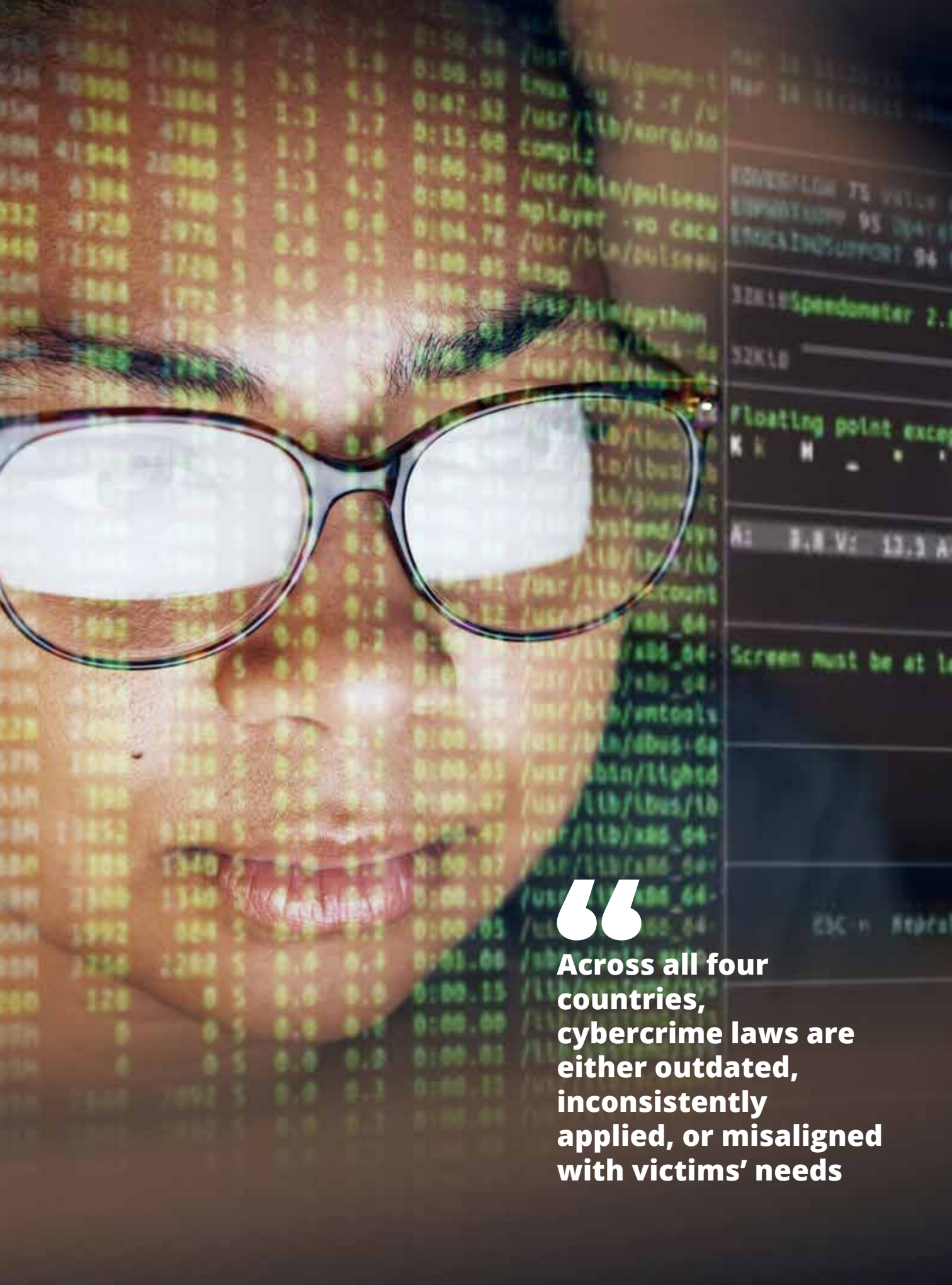
Earlier this year, UNICRI published a report on Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa. Through this research UNICRI sought not only to identify the types of cybercrimes occurring in Africa, but more importantly to understand how people are being affected, and why so many remain without access to justice. Grounded in field visits, stakeholder consultations, and contextual research across East, Southern, and West Africa, the report unpacked the realties on the ground: first, a wide range of cybercrimes are prevalent across the regions; second, not all cybercrimes and online harms are treated equally, with responses often shaped by gendered dynamics; and third, deep structural barriers continue to obstruct access to justice, particularly for those most affected. This research underscored the urgent need to reimagine cybercrime not just as a technical threat, but as a justice issue, one that demands rights-based responses and systemic redesign.

Barrier to accessing justice

Having visited Uganda, Namibia, South Africa, and Sierra Leone, and despite differences in legal frameworks and institutional capacity, a common thread ran through each context: barriers to justice are widespread. Four key challenges emerged across the countries studied:

Outdated or inadequate legal frameworks

Across all four countries, cybercrime laws are either outdated, inconsistently applied, or misaligned with victims' needs. Namibia's Cybercrime Bill has been under discussion for nearly a decade, leaving a legal vacuum. South Africa has more advanced legislation, but frontline responders often lack clarity on how to record or respond to cybercrime reports. Sierra Leone's Cybersecurity and Crime Act is a welcome development, yet its effectiveness remains largely untested, with no finalised cases at the time of writing. In Uganda, stakeholders raised concerns that the law disproportionately targets government critics while offer-



“Across all four countries, cybercrime laws are either outdated, inconsistently applied, or misaligned with victims’ needs

ing limited protection or recourse for victims. These gaps not only undermine accountability but risk enabling misuse of legal tools, leaving victims without meaningful justice.

Capacity constraints

Law enforcement and justice systems across the region face significant resource and training deficits. Officers often lack the tools and technical knowledge to investigate and prosecute cybercrimes effectively. In Namibia, police training curricula exclude cybercrime and basic digital literacy, leaving officers ill-equipped to handle complex or sensitive cases, including online child sexual exploitation. Uganda faces similar challenges, with some police stations lacking even basic equipment like computers. The broader justice system also fails to integrate cybersecurity awareness. In South Africa, concerns were raised that judges are not receiving adequate training to properly navigate the nuances of cybercrimes. Sierra Leone has made strides through collaborative training efforts, but prosecutors still struggle to secure convictions due to weak investigations and insufficient evidence. These capacity gaps erode trust and deter victims from seeking help.

Knowledge gaps

Victims and frontline responders alike struggle to navigate existing mechanisms for redress.

> **“Many officers lack the specific skills and resources required to handle cybercrime cases, especially at the early stages of reporting where victims often seek immediate support.”**

For example, in South Africa, many police officers are not equipped with the knowledge to properly categorise and code cybercrimes that are reported. In Namibia underreporting is driven by a lack of knowledge; digital illiteracy; shame; perception of a lack of responsiveness from police and fears of re-victimisation. Although the Sierra Leone’s Cyber Security and Crime Act has been in place for several years, the police estimate that 70% of people remain unaware of its provisions or where to report cybercrime.

Low public awareness

Cybercrime is still poorly understood by the general public, particularly when it comes to personal or gendered harms such as online harassment and image-based abuse. Many people do not recognise these experiences as crimes, nor are they aware of their rights or available remedies. This lack of awareness contributes to underreporting and perpetuates impunity.

Designing for justice: six practical solutions

These challenges are widespread and contribute to persistent rights violations, but they are not beyond repair. With thoughtful redesign and systems that centre victims' needs, meaningful and accessible pathways to justice can be built. While some reforms demand deeper structural change, such as legislative reform, many practical improvements are within more immediate reach. Both must be pursued with urgency. UNICRI's report outlines a series of actionable solutions that can strengthen cybercrime response and advance justice for those most affected. Each of these reforms reflects a justice-by-design approach: practical, inclusive, and centred on victims lived realities.

Embark on law reform efforts: Cybercrime laws must be rights-based, clear, enforceable, and victim-centred. Vague definitions create loopholes and risk misuse, including silencing dissent. Strong legal frameworks help unlock budgets, guide enforcement, and build trust. Legislative clarity also enables better tools, training, and systems to protect victims.

Simplify reporting pathways: Victims need easy, trusted ways to report cybercrime. That means clear processes, trained responders, and user-friendly tools, like WhatsApp bots, hotlines, and online portals with step-by-step guidance. Reporting must be intuitive and accessible, especially for gendered harms.

Standardise cybercrime coding: Without consistent coding, cybercrimes can go untracked and unaddressed.

> **"Countries must develop clear, locally relevant systems to classify and record digital harms."**

These should be co-designed by justice sector actors, and backed by training. Public-facing versions should use plain language so victims can identify and report crimes.

Create practical SOPs: Police need clear, step-by-step guidelines for handling cybercrime. Standard Operating Procedures (SOPs) should cover everything from intake to investigation, with a focus on consistency, efficiency, and victim care. SOPs must be trauma-informed, rights-based, and easy to use.

Train justice sector stakeholders: Training is essential. Police, prosecutors, and judges must understand cybercrime, digital evidence, and victim-sensitive approaches. Programmes should be rights-based, focused on access to justice, practical, and tailored to emerging threats.

Launch a "Know Your Rights" campaign: Public awareness is power. A "Know Your Rights" campaign can help people recognise cybercrime, understand their options, and know where to seek help. It can tackle stigma, especially around gendered harms and promote digital safety.

These practical and realisable solutions are well within reach. It requires us to start off by simply shifting the narrative: cybercrimes must be understood not only as a technical or security issue, but as a human rights and justice issue.

It then requires some redesign. Across Uganda, Namibia, South Africa, and Sierra Leone, the barriers to justice are real, but they are not immovable. By embedding justice into the design of laws, systems, and institutions, we can shift from reactive enforcement to proactive protection. This means centring victims, simplifying access, and building capacity across the justice cycle.

> **"Justice by design is not a slogan, it is a blueprint for action. It calls on policymakers, practitioners, and communities to reimagine cybercrime responses as pathways to dignity, accountability, and inclusion."**

With urgency and collaboration, Africa can lead the way in crafting digital systems that protect rights, restore trust, and deliver justice where it's needed most.

About the Author

Tina Power is an Attorney of the High Court of South Africa and a Director of ALT Advisory - an African-rooted collective of public interest lawyers, researchers, and technologists working for positive social change. Tina works on advancing digital rights through research, policy reform, and strategic litigation across domestic, regional, and international contexts, having worked in over 25 countries. She regularly consults to various UN agencies and recently supported UNICRI with its report on Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa. Tina has experience in human rights advocacy, research and training with a focus on access to justice, online harms reduction, and the promotion of equality, non-discrimination, and free expression both on and offline. Tina has worked closely with victims and survivors of cybercrimes, as well as activists, journalists, and international institutions. She holds an LLM in Human Rights Advocacy and Litigation from the University of the Witwatersrand and an MSc in International Human Rights Law from Oxford University.

Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa

This new report explores how cybercrime is impacting access to justice in four African countries (Namibia, Sierra Leone, South Africa and Uganda) and offers a broader perspective on challenges and responses across the continent. It highlights the pressing need for national and regional responses that are inclusive, coordinated and evidence-based.

Download the publication