RFLD

PAN-AFRICAN GENDER JUSTICE & RESEARCH NETWORK

PAN-AFRICAN LEGAL RESOURCE

RFLD Legal Toolkit: Cyber Harassment

A Practical Guide for WHRDs, Journalists, Activists, NGOs, Sexual Minorities, Lawyers, and Victims of Digital Violence.

Operating in 55 African Countries

156,000+ Leaders Network

2026 Edition

PROTECT

DEFEND

INTRODUCTION

About RFLD: Pan-African Network

Established 2012, Feminist Leadership

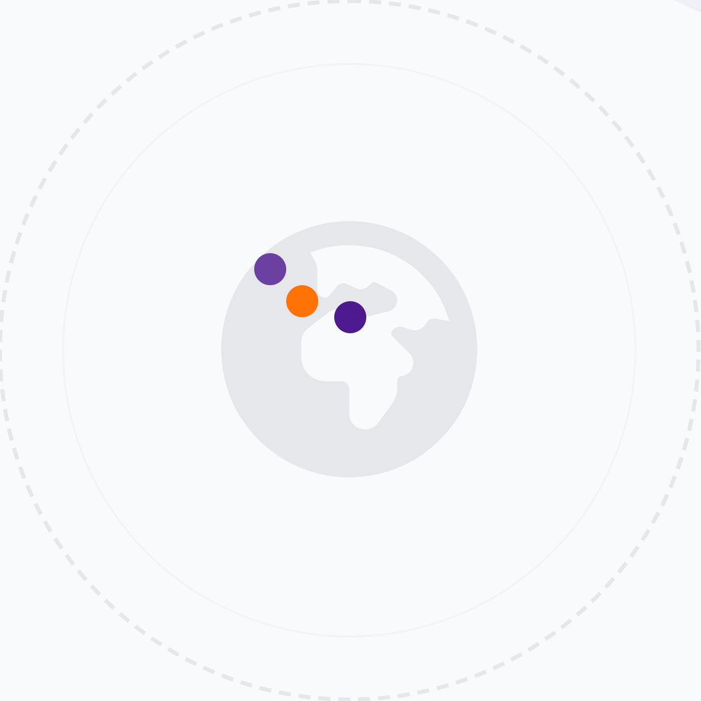
Founded to advance women's rights and political power through integrated systems change across the continent.

ACHPR Observer Status Recognized

Officially accredited by the African Commission on Human and Peoples' Rights to monitor and report violations.

Offices: Ghana, Benin, Gambia

Strategic regional hubs coordinating operations, protection programs, and advocacy across West Africa and beyond.



55

COUNTRIES COVERED

NETWORK IMPACT

RFLD Reach & Leadership Network

Active in 55 African Countries

A truly continental presence spanning West, East, Central, Southern, and North Africa, ensuring diverse regional representation.

156,000 Trained Leaders

Empowering a vast network of Women Human Rights Defenders, journalists, and activists equipped with legal and digital skills.

Community-Led Change

Solutions are owned and driven by local beneficiaries who transition into decision-makers and advocates within their own communities.

156K

ACTIVE LEADERS

CONTEXT OVERVIEW

Digital Violence Crisis in Africa

Escalating, Gendered Online Abuse Patterns

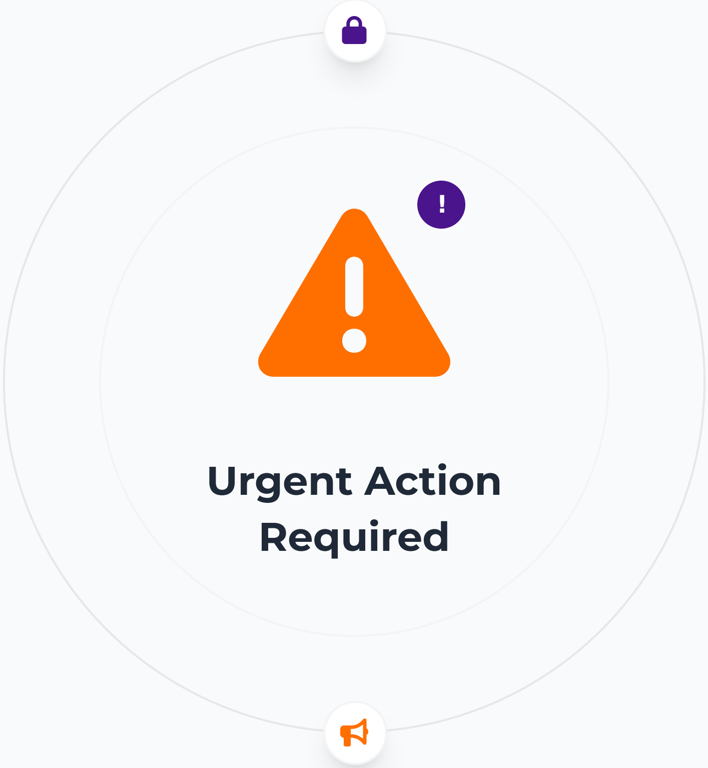
Women and marginalized groups face disproportionate, coordinated attacks designed to intimidate and silence.

Harms Rights, Safety, Participation

Digital violence infringes on freedom of expression and physical safety, forcing women out of public discourse.

Limited Reporting and Weak Enforcement

Existing legal mechanisms are often inadequate, leaving victims without effective recourse or justice.



Urgent Action Required

TARGET AUDIENCE

Who This Toolkit Is Designed For

WHRDs Facing Coordinated Attacks

Women Human Rights Defenders dealing with systematic harassment, threats, and intimidation campaigns online.

Journalists, Activists, NGO Staff

Professionals and advocates operating in digital civic spaces who face gendered retaliation for their work.

Sexual Minorities, Youth, Lawyers

Vulnerable groups needing specific protections and legal professionals seeking to defend victims of digital violence.

Comprehensive Support

Providing legal, digital, and psychosocial resources

DEFINITION

What Is Cyber Harassment?

Persistent Targeted Online Abuse

Intentional, repeated aggressive behavior directed at specific individuals or groups to cause distress or silence them.

Uses Platforms, Devices, Networks

Exploits social media, messaging apps, email, and mobile networks to reach victims across digital spaces.

Causes Fear, Harm, Silencing

Results in severe psychological distress, reputational damage, and withdrawal from public discourse and activism.

Definition

UNDERSTANDING THE SCOPE

DEFINITIONS

Technology-Facilitated Gender-Based Violence

Violence Enabled Through Technology

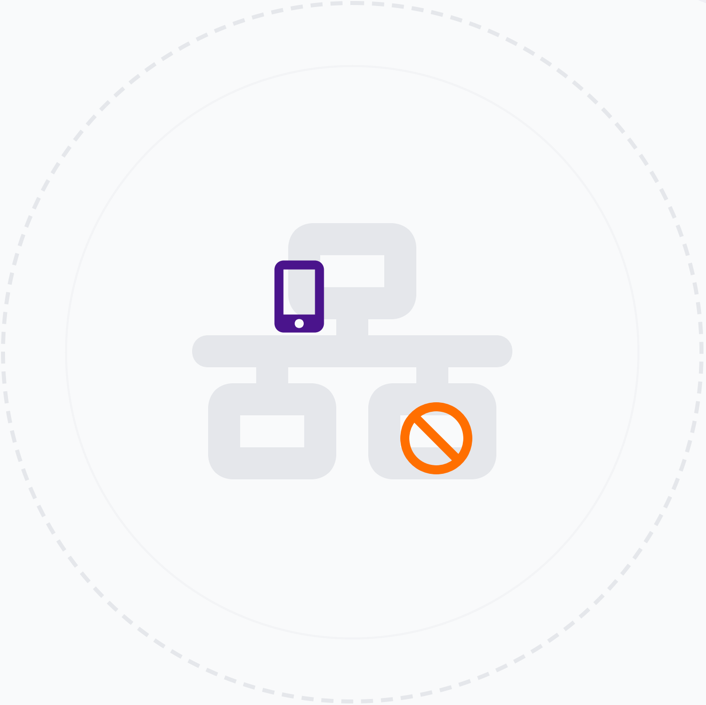
Any act of gender-based violence committed, assisted, aggravated, or amplified using ICTs and digital tools.

Includes Stalking, Threats, Exposure

Encompasses a wide spectrum of harms from cyberstalking and death threats to non-consensual image distribution.

Gendered, Intersectional, Pervasive

Disproportionately targets women and girls, with compounded impacts based on race, sexuality, and disability.



TFGBV

ONLINE & OFFLINE CONTINUUM

UNDERSTANDING DIGITAL VIOLENCE

Why Women Are Targeted Online

Patriarchy and Entrenched Misogyny

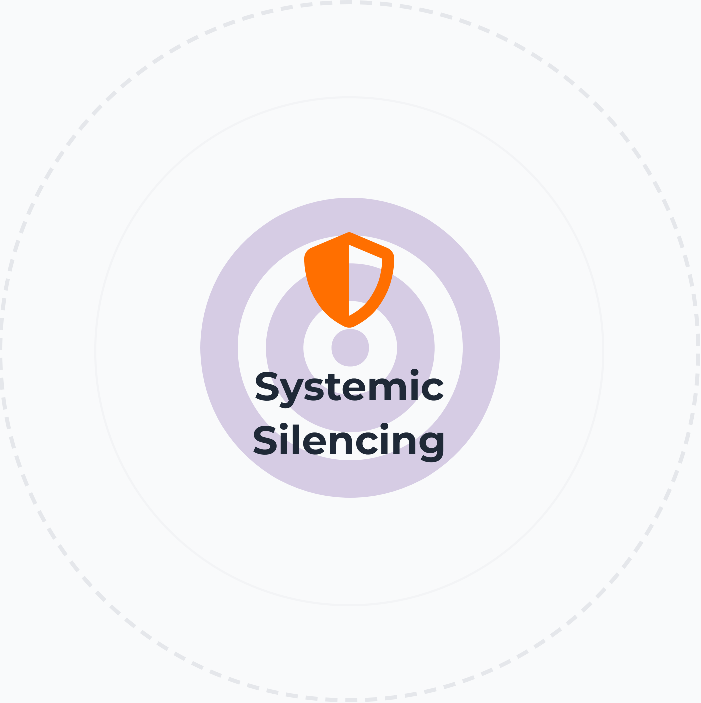
Online spaces often mirror offline inequalities, where existing power dynamics and gender biases are amplified through digital platforms.

Backlash Against Women's Leadership

Women who occupy public spaces or leadership roles face targeted attacks aimed at silencing their voices and discouraging participation.

Coordinated Disinformation & Brigading

Organized campaigns use bots and trolls to overwhelm targets with hate speech, threats, and false narratives to undermine credibility.



Systemic Silencing

"Attacks are designed not just to hurt, but to exclude women from public discourse."

GLOBAL & REGIONAL DATA

Scale of the Problem: Digital Violence Statistics

73% Global

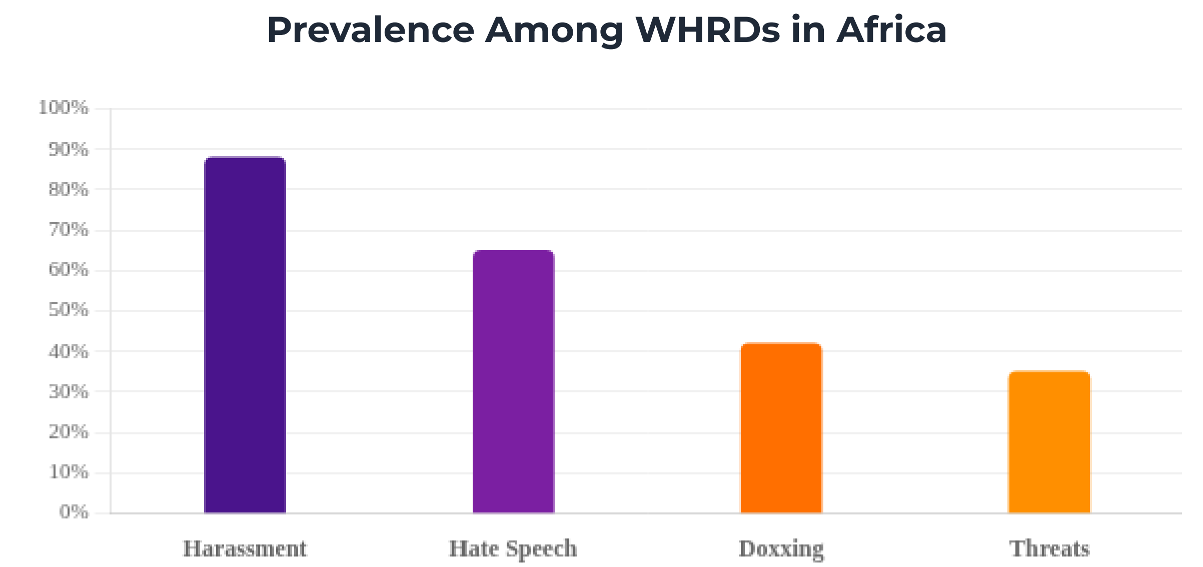
Women Journalists Targeted

Of women journalists surveyed globally have experienced online violence in the course of their work.

8.2M Impacted

Women Reached by RFLD

African women directly impacted through RFLD's protection programs and legislative advocacy.



90%

INCIDENTS UNDERREPORTED

12

GOVS CITING RFLD DATA

Sources: UN Women Global Survey (2022), RFLD Data Center (2025), UNESCO "The Chilling" Report.

SECTION 2: UNDERSTANDING DIGITAL VIOLENCE

Impact on Rights and Democracy

Chills Free Expression and Participation

Digital violence silences critical voices, forcing women and marginalized groups to withdraw from public discourse and political debates.

Undermines Media Freedom and Accountability

Targeted attacks on journalists erode press freedom, leading to self-censorship and reducing investigative reporting on corruption and rights.

Erodes Civic Trust and Safety

Widespread online abuse creates a hostile environment that diminishes public trust in democratic institutions and discourages

Democratic Erosion

When voices are silenced, democracy weakens.

TYPES OF CYBER HARASSMENT

Type 1: Harassment and Trolling

Mass Replies, Insults, Pile-ons

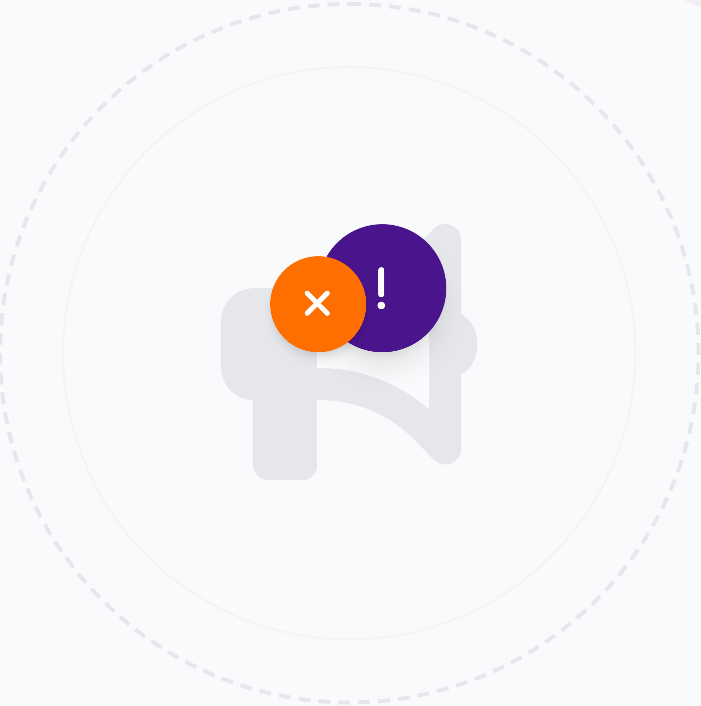
Overwhelming volume of abusive messages designed to intimidate, distract, and silence targets through sheer quantity.

Dogpiling and Coordinated Campaigns

Organized attacks where multiple accounts simultaneously target an individual, often incited by influential figures.

Persistent, Time-Bound Abuse Waves

Sustained periods of harassment that spike during specific events or activism, creating predictable cycles of abuse.



Trolling

ONLINE HARASSMENT

TYPES OF CYBER HARASSMENT

Type 2: Doxxing Private Information

Publishing Personal Data Without Consent

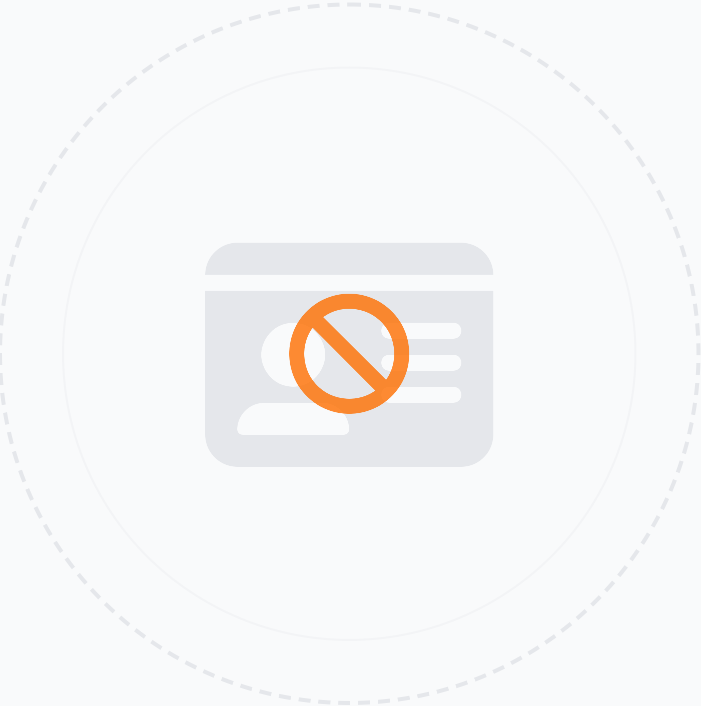
Malicious release of private identifying information online with intent to harm, intimidate, or punish targets.

Addresses, Phones, Family Details Exposed

Sharing home addresses, phone numbers, ID documents, or family member details to incite harassment.

Facilitates Offline Threats and Stalking

Moves digital violence into physical spaces, creating immediate safety risks and potential for real-world attacks.



Privacy Breach

HIGH RISK IMPACT

TYPES OF CYBER HARASSMENT

Type 3: Non-Consensual Intimate Images

Sharing Without Consent

The distribution of private, sexually explicit images or videos without the depicted person's permission (often called "revenge porn").

Blackmail and Extortion

Used as a tool for coercive control, threatening exposure to silence victims, force compliance, or demand money.

Severe Trauma and Harm

Causes devastating psychological impact, social stigma, and long-term reputational damage affecting personal and professional life.

Digital Rights Violation

PRIVACY & DIGNITY

TYPES OF CYBER HARASSMENT

Type 4: Cyberstalking and Surveillance

Repeated Monitoring and Unwanted Contact

Continuous tracking of online activity, persistent messaging across multiple platforms despite blocking, and creating fear through omnipresence.

Spyware, Stalkerware, and GPS Misuse

Installation of malicious software to access private data, track real-time location via GPS, and monitor communications without consent.

Pattern of Fear and Control

24/7

INTRUSIVE MONITORING

TYPES OF CYBER HARASSMENT

Type 5: Impersonation & Fake Accounts

Clone Profiles & Deepfakes

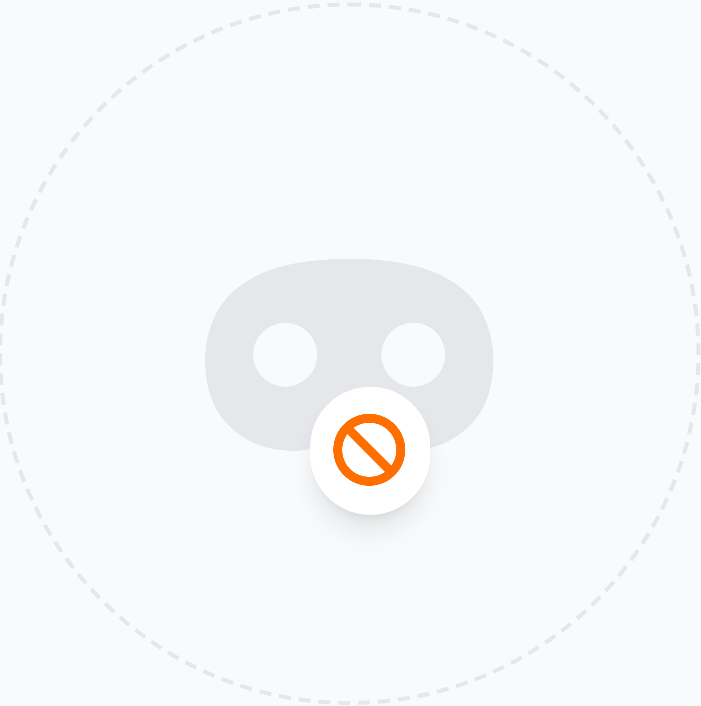
Creating identical social media profiles or using AI-generated media to steal identity and deceive networks.

False Statements & Damage

Impostors posting controversial or harmful content to deliberately destroy professional and personal reputation.

Phishing & Fraud

Using fake identities to extract sensitive information, money, or access credentials from family and colleagues.



Identity Theft

DIGITAL FRAUD

UNDERSTANDING DIGITAL VIOLENCE

Type 6: Targeted Disinformation Campaigns

Smears, Edited Content, Strategic Lies

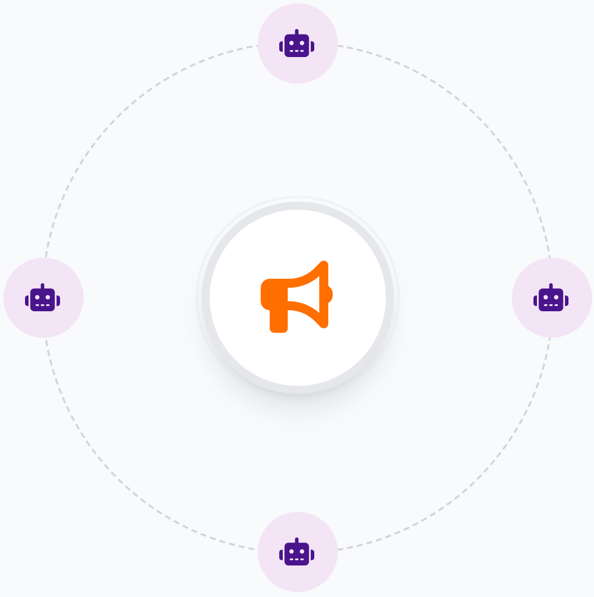
Fabricated stories, deepfakes, and manipulated media specifically designed to destroy reputation and credibility.

Bots Amplify Misogynistic Narratives

Automated bot networks artificially inflate hate speech to create a false appearance of public consensus.

Politically Motivated Silencing Tactics

Strategic attacks often timed to suppress critical reporting, activism, or women's political participation.



Truth Distortion

Disinformation Ecosystem

TYPES OF CYBER HARASSMENT

Type 7:
Threats of Violence & Rape

Explicit Threats of Physical Harm

Direct, specific statements of intent to cause bodily injury, death, or severe physical suffering to the target or loved ones.

Graphic Messages and Intimidation

Sending violent imagery, detailed descriptions of sexual assault, or gore to instill immediate fear and psychological trauma.

Incitement from Extremist Groups

Calls to action by radical networks urging followers to attack specific women defenders, often escalating from online to offline risk.

Immediate Action Required

Report to Police & Secure Safety

TYPES OF CYBER HARASSMENT

Type 8: Hate Speech & Discrimination

Sexist, Homophobic, Transphobic Slurs

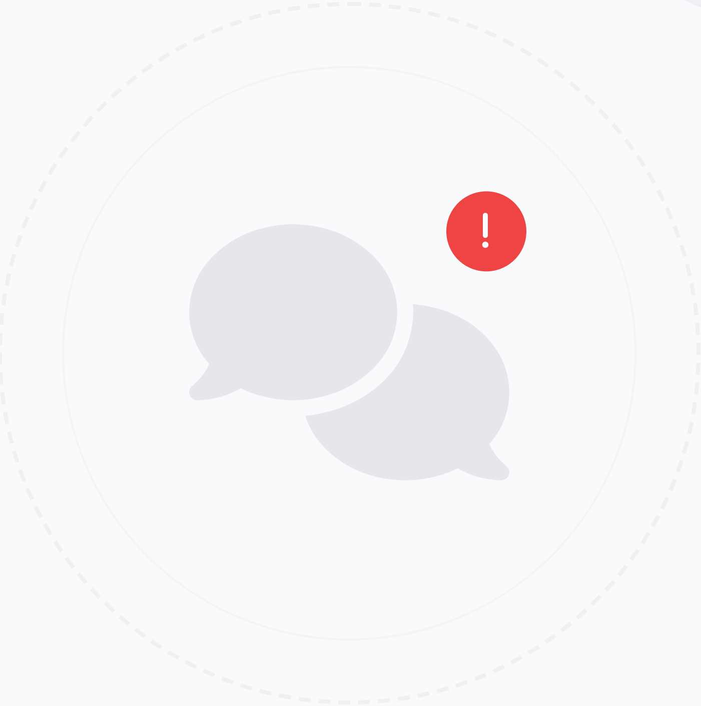
Using dehumanizing language and derogatory terms targeting gender, sexual orientation, or gender identity to attack dignity.

Racist, Xenophobic, Intersectional Abuse

Targeting individuals based on race, ethnicity, or nationality alongside gender, creating compounded harms and exclusion.

Violates Platform Rules and Laws

Often breaches community guidelines and national hate speech legislation, providing grounds for reporting and legal action.



Zero Tolerance

FOR ONLINE HATE

IMPACT ON VICTIMS

Psychological Impact: Mental Health

Anxiety, Depression, Trauma Symptoms

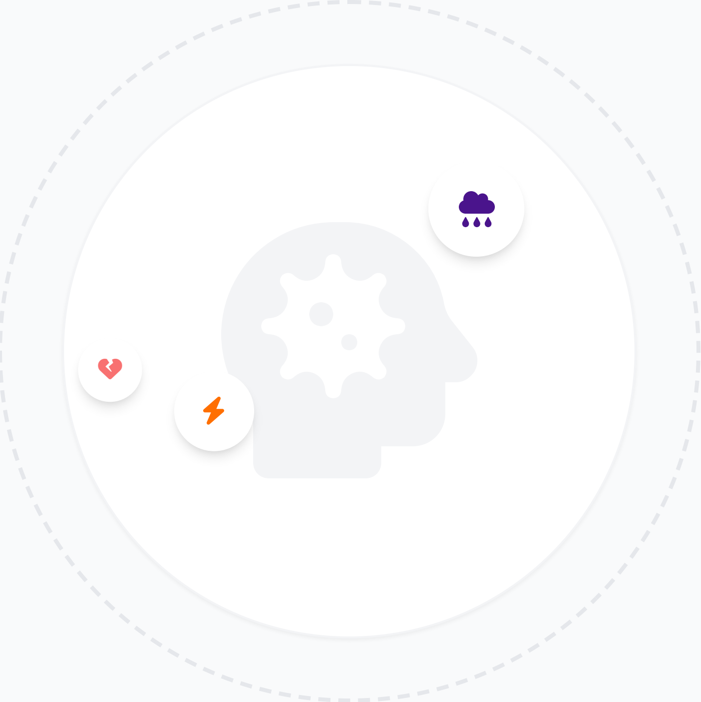
Victims often experience severe anxiety disorders, clinical depression, and symptoms consistent with PTSD following targeted harassment.

Hypervigilance, Sleep Disruption, Fear

Constant state of alertness, chronic insomnia, and pervasive fear for personal safety disrupt daily functioning and wellbeing.

Isolation and Self-Censorship Patterns

Withdrawal from social networks and self-censorship as a coping mechanism leads to professional and personal isolation.



Invisible Scars

LONG-TERM CONSEQUENCES

IMPACT ON VICTIMS

Professional Impact: Career Harm

Lost Opportunities and Assignments

Victims often lose contracts, speaking engagements, and crucial assignments due to coordinated smear campaigns.

Self-Censoring Public Commentary

Fear of further attacks forces professionals to withdraw from public debates, limiting their influence and voice.

Damaged Credibility and Setbacks

False narratives and reputational damage lead to long-term career setbacks and loss of professional trust.

High

ECONOMIC COST

IMPACT ON VICTIMS

Physical Safety Risks: Real-World Danger

Stalking Escalating to Offline Harm

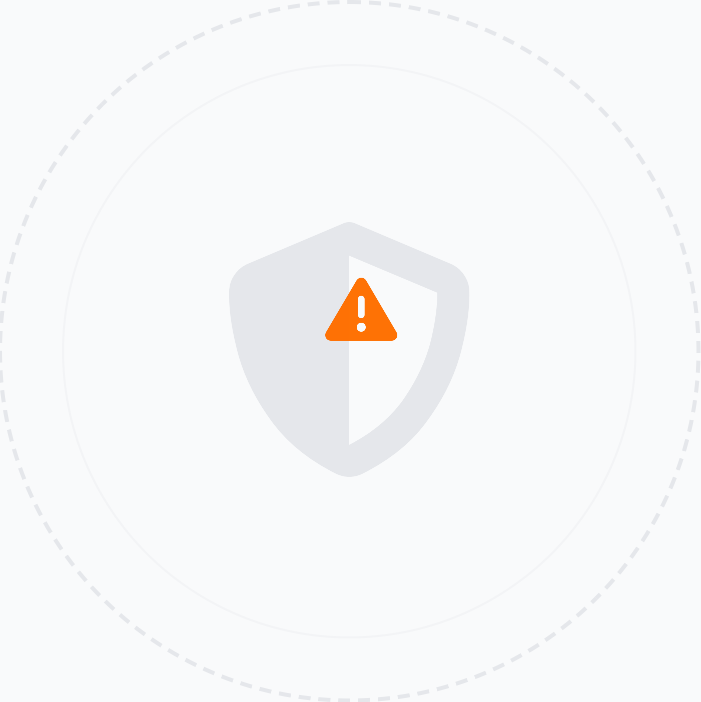
Digital surveillance often precedes physical stalking, enabling perpetrators to track movements and locations in real-time.

Mob Attacks Following Doxxing

Publication of home addresses or workplaces can trigger coordinated physical harassment or violent confrontations by online mobs.

Family Members Targeted by Attackers

Perpetrators frequently threaten or harm children, spouses, and relatives to intimidate and silence the primary target.



Real Danger

ONLINE TO OFFLINE

IMPACT ON VICTIMS

Economic Consequences

Legal Fees and Security Costs

Significant financial burden from hiring counsel, improving digital security, and implementing physical protection measures.

Lost Income and Employment Instability

Forced resignation, termination due to reputational damage, or inability to work due to trauma and harassment.

Demonetization and Advertiser Pullback

Journalists and creators face revenue loss when platforms demonetize content flagged by mass reporting campaigns.

COST OF SILENCE

IMPACT ON VICTIMS

Silencing Effect on Activism

Reduced Advocacy

Constant harassment forces activists to retreat from public spaces, significantly reducing their capacity to advocate for human rights.

Movement Fragmentation

Sustained pressure and attacks create divisions and fear within movements, weakening collective organizing and solidarity efforts.

Fewer Women in Debates

The toxic online environment drives women and marginalized voices out of crucial public debates, impoverishing democratic discourse.

Democratic Deficit

LOSS OF VOICES

IMPACT ANALYSIS

Impact on Sexual Minorities

Outing Campaigns and Blackmail

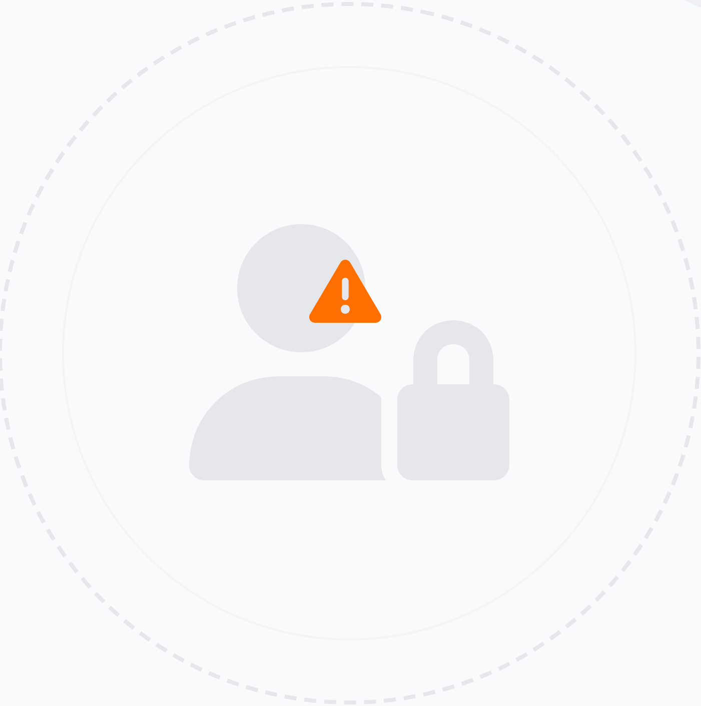
Malicious exposure of sexual orientation or gender identity, often used for extortion or to incite community violence.

Arrests Under Discriminatory Laws

Digital evidence is frequently weaponized by authorities to prosecute individuals under anti-LGBTIQ+ legislation.

Unique Community Safety Challenges

Requires specific digital security protocols due to heightened risks of entrapment and physical retaliation.



High Risk

TARGETED SURVEILLANCE

INTERNATIONAL LAW

UDHR: Foundational Human Rights

Dignity, Equality, Security Rights

Fundamental right to live free from violence, discrimination, and fear applies equally in digital spaces.

Expression and Privacy Protections

Article 12 protects against arbitrary interference with privacy, family, home, or correspondence.

Online and Offline Rights Continuum

Rights protected offline must also be protected online, as affirmed by UN

ARTICLE 1

"All human beings are born free and equal in dignity and rights."

ADOPTED 1948

INTERNATIONAL CONVENTION

CEDAW: Eliminating Discrimination

States Prevent GBV

Obligation to eliminate discrimination includes preventing gender-based violence in all forms.

Address Digital Harms

General Recommendation No. 35 explicitly recognizes technology-facilitated violence against women.

Ensure Effective Remedies

States must provide accessible legal pathways for survivors to seek justice

WOMEN'S BILL OF RIGHTS

"Discrimination against women violates the principles of equality of rights and respect for human dignity."

ADOPTED 1979

INTERNATIONAL LAW

UN HRC: Human Rights Council Resolutions

Condemn Online Violence

Strongly condemn all forms of gender-based violence, including online and ICT-facilitated violence against women globally.

State Accountability

Call for effective state accountability measures to prevent, investigate, and prosecute online gender-based violence.

Resolution 38/5

"Preventing and eliminating violence against women and girls in digital contexts."

ADOPTED 2018

INTERNATIONAL LAW

UN Special Rapporteur: Violence Against Women

Reports on TFGBV

Consistently documents how technology-facilitated violence disproportionately harms women and girls globally.

Prevention Guidance

Provides authoritative frameworks for preventing online violence and protecting digital spaces for women.

State Recommendations

Issues specific calls to action for states and tech platforms to ensure

MANDATE

"To seek and receive information on violence against women, its causes and consequences."

ESTABLISHED 1994

UNITED NATIONS

UNESCO:
Journalist Safety Guidelines

Protect from Online Abuse

Member states must ensure journalists can work freely without fear of digital harassment or targeted attacks.

Newsroom Safety Protocols

Media organizations encouraged to implement digital security training and support systems for staff.

Gender-Responsive Approaches

Specific measures required to address disproportionate attacks against

THE SAFETY OF JOURNALISTS

"Online attacks on women journalists are designed to belittle, humiliate, and shame."

UN PLAN OF ACTION

INTERNATIONAL LAW

UN Resolution: Digital Violence Recognition

Recognizes TFGBV Harms

Acknowledges that violence against women and girls is increasingly committed through digital technologies.

Urges Legal Reforms

Calls upon States to adopt concrete measures and laws to combat technology-facilitated violence.

A/HRC/RES/50/18

"Condemning all forms of violence against women and girls... in digital contexts."

ADOPTED 2022

INTERNATIONAL LAW

ICCPR:
Civil and Political Rights

Privacy, Security, Expression

Articles 17 and 19 safeguard privacy and expression, which are essential for digital security and activism.

Proportionate Restrictions

Any limitations on rights must be necessary, lawful, and proportionate, preventing arbitrary censorship.

Protection from Harassment

States have a positive obligation to protect individuals from online

ARTICLE 19

"Everyone shall have the right to freedom of expression... regardless of frontiers."

ADOPTED 1966

INTERNATIONAL LAW

Beijing Platform for Action (1995)

Address Harmful Stereotyping

Strategic objective to combat media stereotypes that degrade women and fuel gender-based violence.

Ensure Equal Access & Safety

Women must have non-discriminatory access to expression and decision-making in media and technologies.

Integrate Digital Safety

Develop regulatory mechanisms and codes of conduct to promote

SECTION J

"Women and the Media: Promote a balanced and non-stereotyped portrayal of women."

SECTION J, PARA 234

REGIONAL INSTRUMENT

African Charter: Rights and Duties

Dignity, Equality, Non-Discrimination

Articles 2, 3 and 5 guarantee every individual the right to respect for dignity and equality before the law.

Expression and Information Rights

Article 9 protects the right to receive information and express opinions within the law.

Freedom from Violence

Implicit protection against physical and psychological harm, extending to

ACHPR

"Every individual shall be entitled to the enjoyment of the rights and freedoms recognized..."

BANJUL CHARTER 1981

AFRICAN REGIONAL LAW

Maputo Protocol: Article 4 Rights

Life, Integrity, Security

Guarantees every woman the right to respect for her life and the integrity and security of her person.

State Duty to Prevent Violence

States must enact and enforce laws to prohibit all forms of violence against women, including unwanted/forced sex.

Applicable to Digital Spaces

Protections extend to online environments, requiring action against cyber

ARTICLE 4

> *"Every woman shall be entitled to respect for her life and the integrity and security of her person."*

PROTOCOL TO THE AFRICAN CHARTER

AFRICAN REGIONAL LAW

ACHPR Resolution 522: Digital Violence

Calls for Comprehensive Legislation

Urges African states to adopt specific laws addressing all forms of technology-facilitated violence against women.

Expand GBV Definitions to Digital

Recognizes that online violence is real violence and must be legally defined as gender-based violence.

Ensure Access to Effective Remedies

Guarantees victims' right to justice, reparations, and protection from

RESOLUTION 522

"Protection of Women Against Digital Violence in Africa"

ADOPTED 2022

AFRICAN MECHANISM

ACHPR:
Special Rapporteur on WHRDs

Monitors Threats Against Defenders

Systematically tracks and documents reprisals, harassment, and violence targeting women human rights defenders across Africa.

Issues Urgent Appeals

Directly intervenes with governments through urgent letters when defenders face imminent danger or digital persecution.

MANDATE

"To seek, receive, examine and act upon information on the situation of human rights defenders in Africa."

ESTABLISHED 2004

REGIONAL JURISDICTION

ECOWAS Court: Digital Rights Redress

Regional Human Rights Redress

Direct access for individuals and NGOs to file complaints about human rights violations by member states.

Litigate Digital Rights

Proven venue for challenging internet shutdowns, censorship, and online freedom of expression violations.

Cross-Border Enforcement

Judgments are binding on member states, offering recourse when national

JURISDICTION

"The Court has jurisdiction to determine cases of violation of human rights that occur in any Member State."

ABUJA, NIGERIA

REGIONAL MECHANISM

African Court:
Human & Peoples' Rights

Regional Remedy for Violations

Serves as a critical judicial body for addressing serious human rights violations across the African continent.

Expression & Safety Precedents

Establishes binding legal precedents protecting freedom of expression and safety for journalists and activists.

State Declaration Required

Direct access for individuals and NGOs requires states to make a special

AfCHPR

"Complementing the protective mandate of the African Commission."

ARUSHA, TANZANIA

REGIONAL FRAMEWORK

EAC Framework: Regional ICT Instruments

Regional ICT & Cybercrime Instruments

Comprehensive frameworks establishing standards for electronic transactions, cybersecurity, and data protection across member states.

Harmonize Protections

Directives requiring alignment of national laws to ensure consistent enforcement practices and legal safeguards against digital harms.

Cross-Border Cooperation

Mechanisms for mutual legal assistance and extradition to combat

EAC REGION

"One People, One Destiny: Integrated Digital Safety."

EAST AFRICAN COMMUNITY

REGIONAL COMMITMENTS

SADC Gender Protocol: Regional Safety Standards

Prevent and Respond to GBV

Comprehensive obligation to enact and enforce legislation prohibiting all forms of gender-based violence.

Include Online Safety Provisions

Explicitly addresses cyber harassment and technology-facilitated abuse within GBV frameworks.

National Action Plan Implementation

Requires member states to develop time-bound action plans with clear

ARTICLE 20

"Parties shall take appropriate measures to prevent and eliminate all forms of gender-based violence."

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY

NATIONAL LAWS

Cybercrime Laws: Overview Across Africa

Most States Enacted Cybercrime Statutes

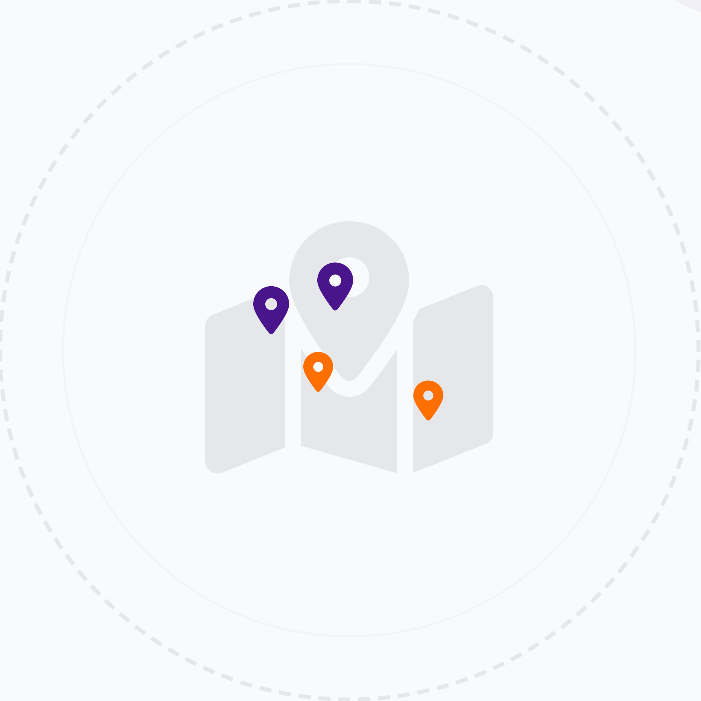
The majority of African nations have passed specific legislation to address digital offenses and online conduct.

Definitions and Protections Vary Significantly

Legal definitions of cyber harassment and available protections differ widely between jurisdictions and regions.

Enforcement Capacity Remains Uneven

Implementation and enforcement mechanisms are inconsistent, often lacking resources or specialized training continent-wide.



30+

NATIONS WITH LAWS

West Africa: Legal Landscape

Key Statutes

- ✓ **Nigeria, Ghana, Senegal**
  Leading nations with specific cybercrime legislation enacted.
- ✓ **Cybercrime & Data Acts**
  Comprehensive frameworks covering digital offenses and data privacy.
- ✓ **Electronic Transactions**
  Laws governing digital commerce and electronic evidence admissibility.

Implementation Reality

- ⚠ **Mixed Enforcement**
  Significant gaps between legal provisions and actual police enforcement.
- ⚠ **Capacity Challenges**
  Limited technical expertise within judicial and investigative bodies.
- ⚠ **Safeguard Concerns**
  Potential for laws to be used against activists without robust safeguards.

East Africa: Legal Protections

Regional Frameworks

- ✓ **Kenya, Uganda, Tanzania**
  Primary jurisdictions with established Computer Misuse Acts.
- ✓ **Cyber Harassment Recognized**
  Specific provisions criminalizing online intimidation and abuse.
- ✓ **Cyberstalking Offenses**
  Laws addressing persistent online monitoring and unwanted contact.

Procedural Mechanisms

- ⚠ **Evidence Procedures**
  Clear protocols for digital evidence admissibility in courts.
- ⚠ **Preservation Orders**
  Legal tools to compel ISPs to preserve critical data.
- ⚠ **Search and Seizure**
  Powers granted to authorities for investigating digital crimes.

Southern Africa: Legislation Status

Key Legislations

- ✓ **South Africa, Zimbabwe, Zambia**
  Primary jurisdictions with enacted cybercrime and data protection laws.
- ✓ **Cybercrimes Act (SA)**
  Comprehensive framework addressing digital offenses and electronic evidence.
- ✓ **Data Protection Acts**
  Strong privacy protections influencing regional legislative trends.

Offenses & Enforcement

- ⚠ **NCII Criminalized**
  Non-consensual intimate image sharing explicitly outlawed in several states.
- ⚠ **Harassment Provisions**
  Specific legal recognition of cyber harassment and stalking behaviors.
- ⚠ **Varied Penalties**
  Wide disparity in sentencing guidelines and procedural enforcement across borders.

North Africa: Legal Context

Key Jurisdictions

- ✓ **Morocco, Tunisia, Egypt**
  Major legal frameworks governing digital space and cybercrime.
- ✓ **Cybercrime Laws**
  Specific legislation addressing digital offenses and electronic evidence.
- ✓ **Surveillance Powers**
  Broad state authority to monitor communications and intercept data.

Specific Risks

- **Speech Restrictions**
  "Morality" and "public order" laws used to prosecute online expression.
- **LGBTQ+ Targeting**
  Cyber provisions frequently weaponized to target sexual minorities.
- **Digital Evidence Misuse**
  Private communications used as evidence in morality-based prosecutions.

EAST AFRICA

Kenya: Computer Misuse Act

A landmark legislative framework establishing specific offenses and procedures for combating digital crimes.

01

Cyber Harassment Defined

Section 27 explicitly criminalizes cyber harassment, imposing fines up to KES 20M or 10 years imprisonment.

Data Preservation Orders

Enables courts to order expedited preservation of data, critical for securing digital evidence before deletion.

Investigative Cooperation

Facilitates mutual legal assistance and police cooperation for cross-border cybercrime investigations.

Legal Impact

Act No. 5 of 2018 provides comprehensive definitions for cyber harassment and unauthorized access.

WEST AFRICA

Nigeria: Cybercrimes Act

The Cybercrimes (Prohibition, Prevention, etc) Act 2015 establishes a comprehensive legal framework.

Legal Impact

Section 24 specifically addresses cyberstalking, criminalizing messages that are grossly offensive or menacing.

01

Cyberstalking Prohibited

Criminalizes sending messages via computer systems that cause annoyance, inconvenience, or fear of death/violence.

●

Service Provider Duty

Mandates service providers to keep traffic data and subscriber information for two years to aid investigations.

●

Jurisdiction & Extradition

Establishes clear jurisdiction for offenses committed in Nigeria or affecting Nigeria, enabling extradition requests.

CHALLENGES

Legal Gaps and Persistent Challenges

Ambiguous Definitions Enable Misuse

Vague terminology like "offensive" or "annoyance" is often weaponized against activists rather than protecting victims.

Overbroad Laws Chill Speech

Excessive penalties and broad scope discourage legitimate expression and self-censorship among defenders.

Weak Victim-Centered Procedures

Lack of trauma-informed protocols and gender sensitivity training results in secondary victimization during reporting.

GAP

IMPLEMENTATION FAILURE

RIGHTS OF SPECIFIC GROUPS

WHRDs: Special Status and Needs

Targeted for Gender Equality Work

Women Human Rights Defenders face unique, compounded risks specifically due to challenging patriarchal norms and structures.

Require Gender-Responsive Protections

Standard security measures are insufficient; tailored approaches addressing sexualized violence and family threats are essential.

International Recognition and Support

UN and African Commission resolutions formally acknowledge WHRDs' distinct status, mandating specific state obligations for their safety.

Gender
Activism
Intersection of Risk

RIGHTS OF SPECIFIC GROUPS

WHRD Protection Mechanisms

Emergency Assistance & Safe Relocation

Immediate support for defenders facing imminent threats, including temporary relocation to safe houses and medical aid.

Digital Security Training & Legal Aid

Capacity building on digital hygiene, secure communication tools, and access to pro-bono legal representation for cyber harassment cases.

Rapid Response Networks & Hotlines

Activated regional networks for urgent mobilization, solidarity statements, and 24/7 emergency hotlines for incident reporting.

Safety

FIRST RESPONSE

SPECIFIC GROUPS

Journalists:
Press Freedom Online

Safety Protocols for Online Harassment

Proactive digital hygiene and established response plans to mitigate coordinated attacks against reporters.

Source Protection Using Strong Encryption

Essential rights to maintain confidentiality of whistleblowers and vulnerable sources through encrypted channels.

Newsroom Reporting and Escalation Pathways

Institutional support mechanisms ensuring journalists can safely report abuse to management for legal action.

Press Freedom

DIGITAL SAFETY

RIGHTS OF SPECIFIC GROUPS

Activist Rights: Digital Spaces

Freedom of Association Online

The right to form, join, and participate in digital groups and movements without interference or persecution.

Expression Against Censorship

Protection against unlawful content removal, internet shutdowns, and silencing of dissenting political speech.

Protection from Surveillance

Safeguards against unlawful monitoring, data interception, and tracking of activist communications and networks.

3

CORE PROTECTIONS

RIGHTS OF SPECIFIC GROUPS

NGO Workers and Civil Society

Organizational Duty of Care Obligations

Employers must proactively protect staff from foreseeable online harms related to their work.

Risk Assessments and Safety Protocols

Conduct regular digital security audits and implement strict protocols for sensitive data handling.

Incident Reporting and Secure Documentation

Establish clear internal channels for reporting threats and securely archiving evidence of attacks.

Duty

OF CARE

SPECIFIC GROUPS

Sexual Minorities: LGBTQ+ Rights Online

Privacy Rights Protect Against Outing

Legal rights to privacy and data protection are critical safeguards against forced outing and digital exposure of sexual orientation.

Challenge Discriminatory Enforcement

Advocacy strategies to contest the misuse of cybercrime laws and digital evidence for prosecuting consensual same-sex conduct.

Community-Led Tailored Safety Strategies

Implementing decentralized, community-specific digital security protocols and peer support networks for resilient protection.

Safety

IN DIGITAL SPACES

SPECIFIC GROUPS

Intersectional Vulnerabilities and Risks

Compounded Risks Across Identities

Women with multiple marginalized identities face amplified, targeted digital violence that is uniquely severe.

Race, Class, Disability Intensify Harms

Discrimination based on ethnicity, economic status, or disability often fuels specific, hateful online attacks.

Tailored, Inclusive Protections Essential

Standard safety measures fail without addressing unique threats faced by diverse groups of women defenders.

Risk+

MULTIPLIED IMPACT

SPECIFIC GROUPS

Youth Activists and Digital Natives

High Exposure to Online Threats

Young activists face disproportionate harassment due to their high visibility on emerging platforms and perceived vulnerability.

Proactive Safety Education

Empowering youth with digital literacy, privacy management skills, and recognizing online grooming or manipulation tactics.

Partnerships with Guardians and Schools

Building support systems involving parents, educators, and institutions to create safer online and offline environments for youth advocacy.

Digital Natives

FUTURE LEADERS

DOCUMENTATION & EVIDENCE

Why Documentation Is Critical

Preserves Proof Before Content Deletion

Evidence often disappears quickly—capturing it immediately ensures you have proof even if perpetrators delete posts or suspend accounts.

Supports Police Investigations and Courts

Verified documentation creates the admissible evidence trail needed for formal complaints, restraining orders, and legal prosecution.

Strengthens Reports to Platforms Effectively

Detailed records with timestamps and context significantly increase the success rate of content takedowns and account suspensions.

Evidence

IS PROTECTION

STEP 01

Take Screenshots Immediately

Digital evidence is volatile. Content can be deleted by perpetrators or platforms within minutes. Securing visual proof is your first priority.

⚠ *Do not block the user before documenting.*

ACTION CHECKLIST

✓ **Capture Full Context**

Screenshot the entire post including the perpetrator's handle, profile photo, and any replies.

✓ **Include Timestamps & URLs**

Ensure the date, time, and browser URL bar are clearly visible in your screenshots.

✓ **Document Ongoing Patterns**

Take screenshots periodically if harassment continues to establish a timeline of abuse.

STEP 02

Record URLs & Usernames

Screenshots are not enough. URLs (web addresses) are the unique fingerprints needed for legal tracking and platform takedown requests.

Unique IDs verify the specific source.

ACTION CHECKLIST

✓ Copy Exact Profile Links

Copy the full URL of the perpetrator's profile page (e.g., twitter.com/username) directly from the browser bar.

✓ Note Post IDs and Permalinks

Right-click the timestamp of the specific abusive post to copy its permanent link (permalink) and unique ID number.

✓ Preserve Hashtags and Group Names

Document exact hashtags used in campaigns and the specific names/URLs of Facebook or WhatsApp groups involved.

STEP 03

Save Original Messages

Beyond screenshots, digital files contain critical metadata that can prove authenticity. Preserve the original message formats whenever possible.

Digital headers act as DNA for online messages.

ACTION CHECKLIST

✓ Export Chats in Original Format

Use platform tools (like WhatsApp's "Export Chat") to download conversation histories as .txt or .html files.

✓ Retain Headers & Metadata

For emails, save the "Show Original" or "View Source" version to capture IP addresses and routing data.

✓ Avoid Editing or Altering Logs

Never modify file names or contents. Forwarding messages changes headers—always save or export directly.

STEP 04

Document Date & Context

Context creates credibility. Isolated incidents may seem minor, but documenting the timing, frequency, and surrounding circumstances proves systematic abuse.

Precision strengthens your legal case.

DOCUMENTATION REQUIREMENTS

✓ Log Chronology Carefully

Record the exact date and time of each incident, noting time zones if the perpetrator is international.

✓ Describe Impact & Witness

Note who saw the abuse, how it affected your work or mental health, and any immediate actions taken.

✓ Note Platform Details

Specify the platform, device used to view it, and your physical location when receiving the threat.

STEP 05

Create Evidence Timeline

A structured timeline turns isolated incidents into a clear pattern of harassment. This is crucial for investigators and legal proceedings to understand the scope.

Chronological order strengthens your case.

ACTION CHECKLIST

✓ **Organize Incidents Sequentially**

List every documented incident by date and time in a spreadsheet or document to show escalation.

✓ **Link Files to Entries**

Reference specific filenames (screenshots, logs) for each entry in your timeline for easy retrieval.

✓ **Summarize Key Events**

Briefly describe the nature of each incident and any escalation points to provide a clear overview.

STEP 06

Store Evidence Securely

Protecting your gathered evidence is crucial for legal proceedings and personal safety. Secure storage prevents tampering, accidental loss, or unauthorized access.

Restrict access to trusted individuals only.

SECURITY MEASURES

✓ Use Encrypted Drives

Store all evidence files on password-protected, encrypted external hard drives or USB sticks to prevent unauthorized access.

✓ Implement Access Controls

Apply strict "least privilege" principles. Only grant file access to legal counsel or essential support team members.

✓ Maintain Offsite Backups

Keep redundant copies in a secure, separate physical location or encrypted cloud storage to protect against device theft or damage.

FINAL STEP

Chain of Custody For Court

To be admissible in legal proceedings, digital evidence must have a documented history of handling. Prove integrity by recording every access and transfer.

Crucial for criminal prosecution success.

VERIFICATION CHECKLIST

✓ **Document Who Handled It**
Create a log identifying every person who collected, accessed, or analyzed the digital evidence files.

✓ **Record Transfers & Storage**
Log dates, times, and methods of transfer between devices or people, and note secure storage locations.

✓ **Maintain Integrity (Hashing)**
Use cryptographic hash functions to verify files haven't been altered or tampered with since collection.

REPORTING MECHANISMS

Where to Report: Overview Map

Police, Platforms, Civil Society Mechanisms

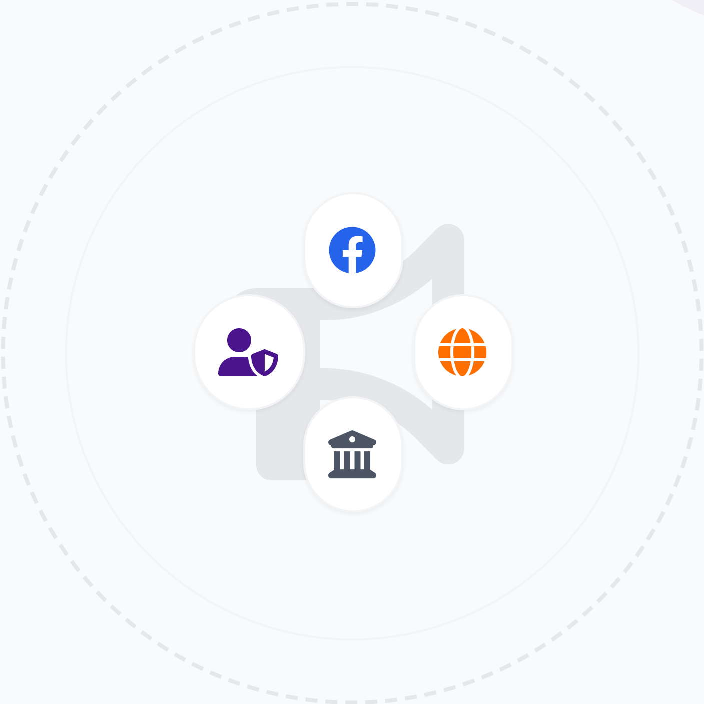
Multi-channel reporting ensures comprehensive documentation and triggers varied protective responses.

National Hotlines and Helplines Directories

Immediate crisis support and local referrals available through verified emergency contact networks.

Regional and International Complaint Bodies

Escalation pathways to ACHPR and UN mechanisms when national remedies are unavailable or exhausted.



3+

PRIMARY CHANNELS

REPORTING MECHANISMS

Reporting to Police: What to Expect

File Detailed Statement with Evidence

Submit a comprehensive written statement including printed screenshots, URLs, and a chronological timeline of incidents.

Obtain Official Reference Case Number

Always demand an official receipt, case number, or OB number to track your report and prove filing.

Request Protection and Safety Measures

Ask specifically for available protection orders, no-contact directives, or emergency safety measures during investigation.

Police Reporting

FORMAL PROCEDURE

LEGAL REMEDIES

Filing Criminal Complaints: Step-by-Step Process

Identify Applicable Offenses

Clearly map the abusive behavior to specific violations in national penal codes or cybercrime acts.

Work With Experienced Counsel

Engage lawyers familiar with digital rights to draft complaints that withstand technical scrutiny.

Follow Up Persistently

Regularly check case status, provide additional evidence, and document all interactions with authorities.

Legal Action

ACCOUNTABILITY MECHANISM

Reporting to **Social Media** Platforms

Effective reporting is key to removing harmful content. Follow these standard protocols to maximize the chances of a successful takedown.

GENERAL REPORTING PROTOCOL

1 **Use In-App Reporting Tools**

Always use the platform's native reporting mechanism first. This generates a ticket ID which is essential for any future escalation.

2 **Cite Violated Policies Clearly**

Identify exactly which community standard was broken (e.g., "Hate Speech," "Non-Consensual Nudity"). Be specific to help moderators.

3 **Request Expedited Review**

For imminent threats or severe doxxing, use trusted partner channels (like RFLD) to escalate the ticket for urgent review.

Pro Tip: *Never rely on a single report. Encourage your support network to report the same content to signal urgency to the algorithm.*

Facebook & Instagram Reporting

Meta platforms have specific tools for dealing with impersonation and harassment. Follow these steps to secure your digital presence.

META PLATFORM PROTOCOLS

1 **Report Harassment & Impersonation**

Go to the profile/post > click three dots (...) > select "Find Support or Report". Specifically choose "Impersonation" or "Harassment" to trigger specialized review flows.

2 **Use Blocking & Privacy Controls**

Utilize "Restrict" mode on Instagram to shadow-ban bullies without notifying them. On Facebook, use "Profile Locking" where available to limit visibility to non-friends.

3 **Request Data Download**

Before content is removed, request a copy of your data (Settings > Your Information) to preserve evidence of harassment for legal proceedings.

Instagram Tip: *Use the "Hidden Words" feature in Privacy settings to automatically filter out comments and DMs containing specific abusive keywords or emojis.*

Reporting on Twitter / X Effectively

Twitter (X) moves fast. Swift reporting of threats and hate speech is critical to stopping viral harassment campaigns before they escalate.

TWITTER / X REPORTING PROTOCOL

1 Report Threats and Hateful Conduct

Use the "Report Post" menu. Select "It's abusive or harmful" and choose specific categories like "Threatening violence" or "Hate speech" accurately.

2 Request Evidence Preservation

If the threat is serious, law enforcement can request X to preserve data. Save the URL and screenshot immediately before reporting as tweets may be deleted.

3 Appeal Wrongful Decisions Promptly

Automated moderation often fails. If you receive a "no violation found" notice, use the appeal link immediately to request human review of the decision.

Safety Tip: *Enable "Quality Filter" and mute notifications from accounts you don't follow to reduce exposure during an attack while reports are processing.*

Reporting: WhatsApp & Telegram

Messaging apps require immediate action to stop harassment and preserve evidence before deletion. Follow these specific steps for encrypted platforms.

MESSAGING APP PROTOCOLS

1 **Report & Block Immediately**

Open the chat info, select "Report Contact" or "Report Spam," then block. This flags the account to the platform's trust and safety systems.

2 **Export Chat History**

Before deleting the chat, use the "Export Chat" feature (without media first, then with media) to create a legally admissible record of abuse.

3 **Engage Abuse Teams**

For severe threats, email screenshots and exported logs directly to abuse@whatsapp.com or abuse@telegram.org with clear subject lines.

⚠ **Critical Warning:** *Do not just delete the chat. Deleting removes evidence permanently. Always archive or export first.*

TikTok & YouTube Reporting

Video platforms require specific actions for harmful content. Act quickly to flag visual evidence and secure your account settings.

VIDEO PLATFORM PROTOCOL

1 **Flag Harmful Videos or Comments**

Use the flag icon below videos. Select specific reasons like "Harassment/Cyberbullying" or "Hateful Content" to trigger review.

2 **Use Safety Mode & Filters**

Enable "Restricted Mode" (YouTube) or "Comment Filters" (TikTok) to automatically hide abusive keywords and protect your feed.

3 **Document Moderation Responses**

Save emails confirming receipt of your report. If rejected, this documentation is vital for escalating to trusted flaggers or partners.

Pro Tip: *On TikTok, use the "Filter all comments" feature during an attack to manually approve comments before they appear publicly.*

LEGAL REMEDIES

Criminal Prosecution Options

Harassment, Threats & Extortion

Charges can be filed for persistent harassment, death threats, and blackmail attempts under national criminal codes.

Cyberstalking, NCII & Hate Crimes

Specific cybercrime laws prosecute stalking, non-consensual image distribution, and targeted hate speech violations.

Victim Protection Orders

Courts can issue immediate restraining orders to prevent further contact or digital violence during investigations.

Legal Action

ENFORCE ACCOUNTABILITY

LEGAL REMEDIES

Civil Lawsuits and Damages

Defamation and Privacy Claims

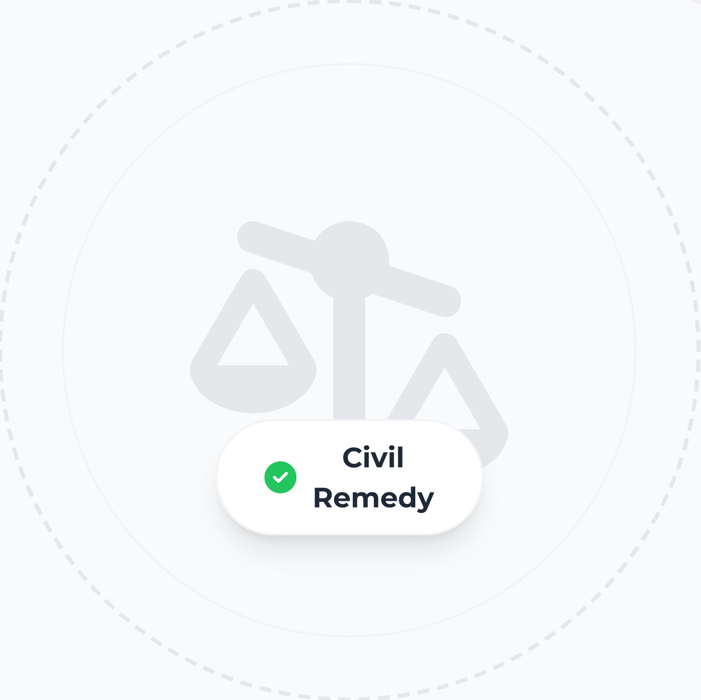
Pursue legal action for libel, slander, or unauthorized disclosure of private facts causing reputational harm.

Intentional Infliction of Distress

Seek redress for severe emotional suffering caused by extreme and outrageous conduct online.

Compensatory and Punitive Damages

Claim financial compensation for actual losses and additional damages to punish malicious conduct.



Civil Liability

LEGAL RECOURSE

LEGAL REMEDIES

Restraining Orders and Injunctions

Protection Orders for Survivor Safety

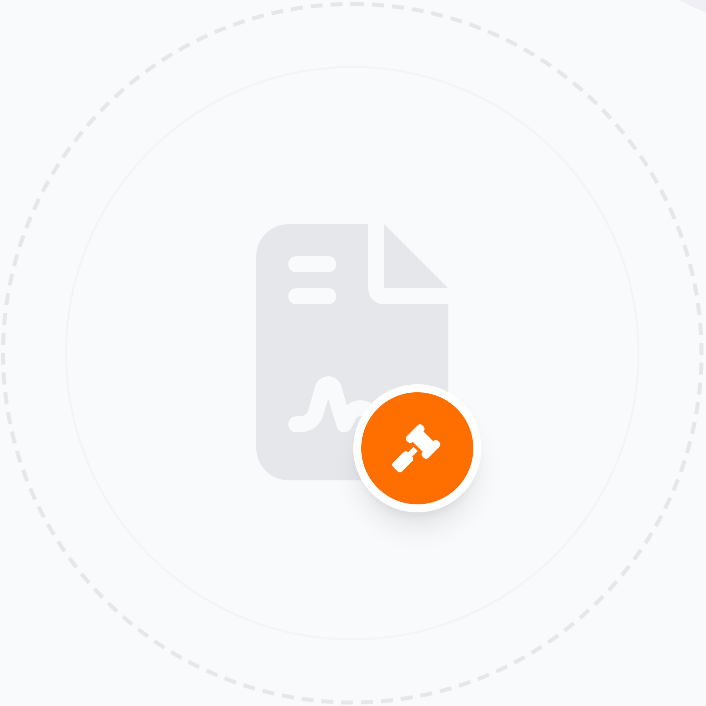
Immediate legal measures to restrict abusers from contacting or approaching victims, ensuring physical and digital safety.

Interim Takedown and No-Contact

Court mandates for rapid removal of harmful content and strict prohibitions against any form of communication.

Enforceable Digital Restrictions

Legally binding orders specifically targeting online behaviors, including blocking access to platforms or devices.



Legal Protection

Ensuring Safety Through Law

LEGAL REMEDIES

Platform Content Removal Pathways

Legal Notices Citing Violations

Issue formal demands to platforms referencing specific terms of service breaches and local law violations.

Court Orders for Compliance

Obtain judicial mandates requiring immediate takedown of illegal content within specific jurisdictions.

Transparency Reporting & Appeals

Utilize escalation channels and public reporting mechanisms to challenge platform inaction or errors.

Takedown

ENFORCEMENT ACTIONS

LEGAL REMEDIES

National Human Rights Commissions

Complaints for Systemic Violations

File detailed reports addressing widespread digital rights abuses that affect communities or groups rather than just individuals.

Mediation and Recommendations

Commissions can facilitate resolution processes and issue formal recommendations to government bodies for corrective action.

Strategic Impact Supporting Reforms

Commission findings create authoritative records that bolster broader advocacy efforts for legal and policy reforms.

Accountability

INDEPENDENT OVERSIGHT

LEGAL REMEDIES

ACHPR Individual Complaint Process

Submit Communication with Evidence

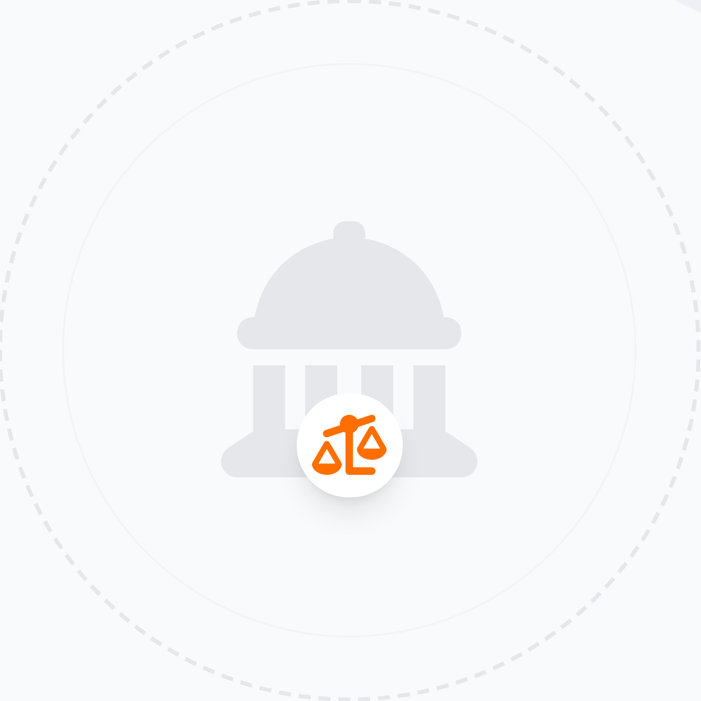
File a formal communication under Article 55 detailing violations with strong, verifiable evidence of the digital violence.

Exhaust Domestic Remedies

Demonstrate that local legal channels were attempted without success, or prove they are unavailable or unduly prolonged.

Request Provisional Measures

Request urgent intervention under Rule 98 to prevent irreparable harm to the victim while the communication is pending.



Art. 55

COMMUNICATIONS

LEGAL REMEDIES

UN Special Procedures Engagement

Write Relevant Special Rapporteurs

Direct submissions to the Special Rapporteur on Violence Against Women and Girls and freedom of expression mandate holders.

Allegations Detailing Facts and Harms

Provide comprehensive factual evidence, timeline of incidents, and specific details on how digital violence impacted rights.

Request Urgent Appeals

Solicit immediate communications to governments demanding cessation of violations and protection for targeted defenders.

SR VAW

SR Expression

SR Defenders

LEGAL REMEDIES

Legal Aid Resources in Africa

Media Defence & Regional Partners

Specialized legal support for journalists and activists facing digital rights violations across the continent.

Bar Associations Pro Bono Rosters

Access free legal representation through national law societies committed to defending human rights cases.

RFLD-Referred Trusted Legal Networks

Verified network of feminist lawyers experienced in handling digital violence and gender-based harassment cases.

Support Available

ACCESS JUSTICE NOW

DIGITAL SECURITY

Prevention Is Your First Defense

Plan, Prepare, Practice Safety

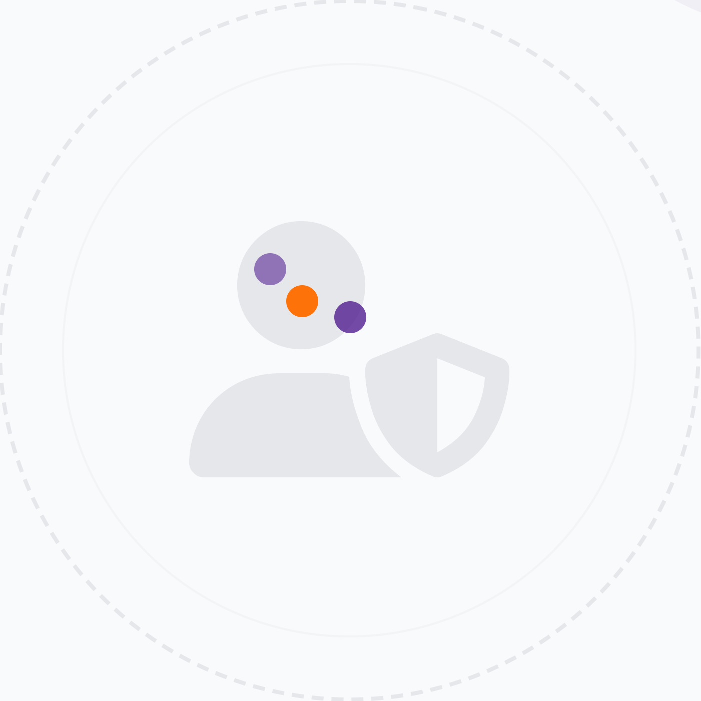
Develop a personal security plan before incidents occur, including regular backups and emergency protocols.

Reduce Digital Attack Surface

Minimize publicly available personal information and restrict account visibility to limit potential exposure.

Respond Quickly and Escalate

Act immediately when threats arise by documenting evidence and engaging support networks without delay.



3

CORE STRATEGIES

DIGITAL SECURITY

Secure Communication: Signal, WhatsApp

Prefer End-to-End Encrypted Apps

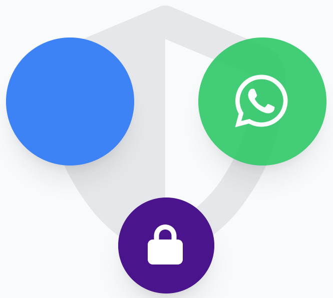
Use Signal or WhatsApp for all sensitive communications to ensure only sender and receiver can read messages.

Verify Safety Numbers with Contacts

Always verify safety numbers or security codes in person or via a secondary channel to prevent man-in-the-middle attacks.

Disable Cloud Backups for Chats

Turn off automatic cloud backups (iCloud/Google Drive) as these are often not end-to-end encrypted and can be subpoenaed.



E2EE

STANDARD PROTOCOL

DIGITAL SECURITY

Privacy Settings on Social Platforms

Restrict Comments and Mentions

Limit who can comment or tag you to strictly trusted contacts to prevent mass harassment.

Limit Audience and Review Tags

Set profiles to private where possible and enable manual review of all tagged content.

Audit App Permissions Regularly

Revoke access for third-party applications that are no longer essential to minimize data leaks.

Control

YOUR DIGITAL FOOTPRINT

DIGITAL SECURITY

Two-Factor Authentication (2FA)

Use App-Based Authenticators Only

Prefer authenticator apps like Google Authenticator or Authy over SMS codes, which are vulnerable to SIM swapping attacks.

Enable on Email and Platforms

Activate 2FA on all critical accounts, especially email, social media, and financial platforms, to prevent unauthorized access.

Store Backup Codes Very Securely

Generate and safely store backup recovery codes offline in case you lose access to your primary authentication device.

99.9%
ATTACKS BLOCKED

DIGITAL SECURITY

VPN Usage for Online Safety

Hide IP and Approximate Location

Prevents tracking of your physical location and masks your digital identity from surveillance.

Use Reputable, Strict No-Log Providers

Ensure your VPN service does not store your browsing history or connection data (e.g., ProtonVPN, Mullvad).

Avoid Free, Untrusted VPN Services

Free VPNs often monetize by selling your data to third parties, defeating the purpose of privacy.

Encrypted Tunnel

SECURE CONNECTION

DIGITAL SECURITY

Password Security
Best Practices

Unique Passwords for Every Account

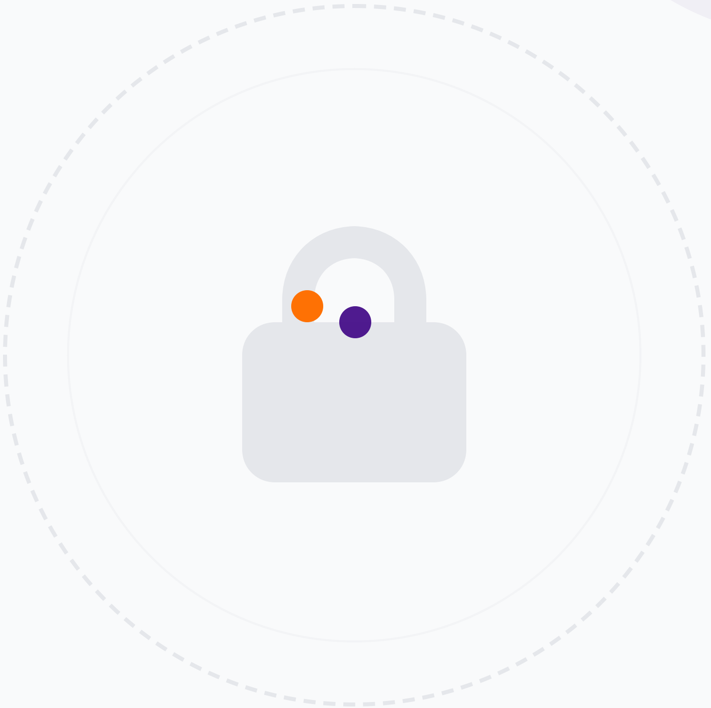
Prevent chain-reaction compromises by ensuring one breach doesn't expose all your online services and data.

Use Reputable Password Manager Software

Generate and store complex, random passwords securely instead of relying on memory or insecure notes.

Enable Breach Monitoring and Alerts

Use tools that notify you immediately if your credentials appear in known data leaks so you can act fast.



Secure

ACCESS CONTROL

DIGITAL SECURITY

Device Security: Phones and Computers

Update Operating Systems & Apps

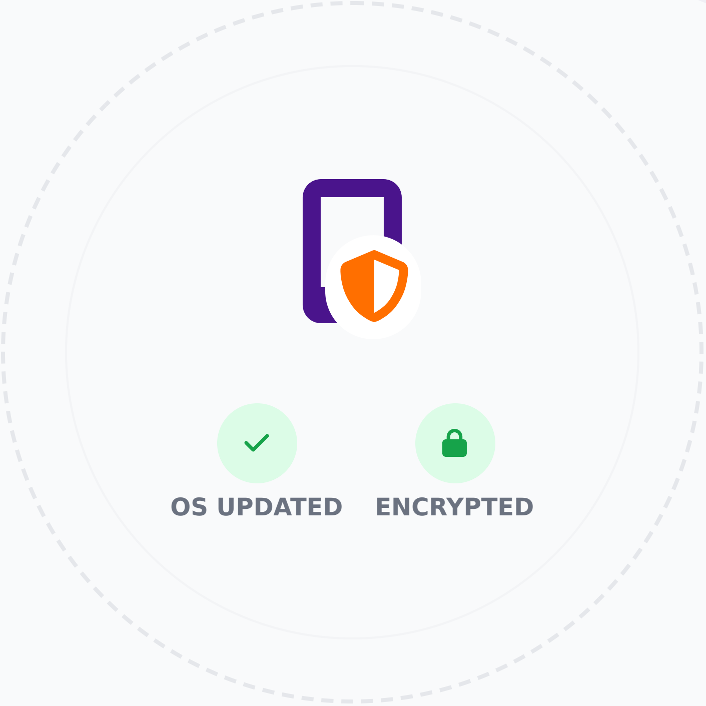
Install security patches immediately to fix vulnerabilities that attackers could exploit to access your data.

Enable Screen Locks & Biometrics

Use strong passcodes, fingerprint, or face ID to prevent unauthorized physical access to your devices.

Encrypt Devices & Secure Backups

Turn on full disk encryption (BitLocker/FileVault) and ensure all backups are password protected.



Device Hardening

Your First Line of Defense

DIGITAL SECURITY

Safe Practices on Social Media

Avoid Geotagging Sensitive Locations

Disable automatic location services and never tag your home, office, or regular meeting spots in real-time posts.

Separate Personal and Public Profiles

Maintain distinct accounts for activism and personal life to limit exposure of family details and private information.

Pause Before Posting Content

Critically review photos and text for inadvertent data leaks like visible documents, street signs, or reflections.

Privacy First

Control what you share to control your safety

Stay Alert

REVIEW PRIVACY SETTINGS

SUPPORT & RESOURCES

RFLD Protection Programs Overview

Emergency Grants and Safe Relocation

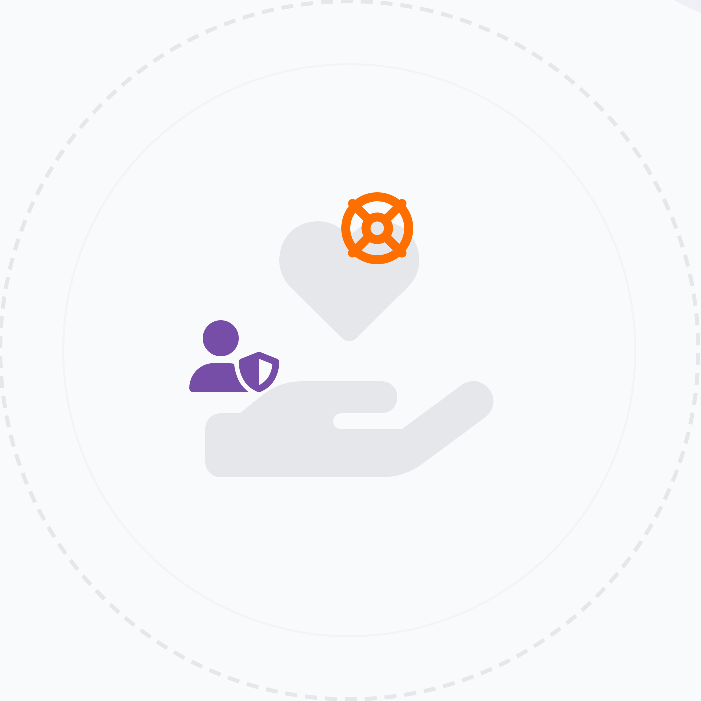
Immediate financial assistance and secure temporary shelter for defenders facing imminent physical danger.

Digital Safety Training Workshops Offered

Hands-on capacity building for organizations and individuals on secure communication and risk mitigation.

Legal Defense and Accompaniment Services

Access to pro bono legal representation and courtroom accompaniment for activists facing judicial persecution.



Holistic

SUPPORT SYSTEM

IMMEDIATE ASSISTANCE

Contact RFLD for Emergency Support

If you are a WHRD, journalist, or activist facing digital violence, our rapid response team is ready to assist you.

Primary Support Email
Monitored 24/7 for high-priority cases

admin@rflgd.org

Response Time: Within 24 Hours for Emergencies

How to Report

1. **Use Clear Subject Line**
Write "URGENT: Digital Violence Emergency - [Your Country]" to flag priority.

2. **Attach Evidence**
Include screenshots, URLs, and a brief timeline. Do not forward malicious links directly.

3. **Secure Communication**
If possible, provide a Signal number or ProtonMail address for secure follow-up.

WEST AFRICA COORDINATION

RFLD Ghana Office Regional Coordination Hub

Our Accra office serves as the central coordination hub for West African programs, providing strategic support and regional oversight.

Central Support Contact

Direct pathway for Ghana-based inquiries

admin@rflgd.org

Hub Services

Coordination Center

Manages regional partnerships and program implementation across Anglophone West Africa.

Support Referrals

Connects local activists with legal aid, psychosocial support, and digital security resources.

Advocacy Leadership

Leads legislative engagement and policy advocacy initiatives within the region.

REGIONAL HUB

RFLD Benin Office Cotonou Hub

Serving Francophone West Africa with specialized legal and digital protection programs for women leaders.

Central Support Email

Main contact point for Benin operations

admin@rflgd.org

Referral Time: 3-5 Business Days

Contact Pathway

1 Email Central Support

Send your inquiry to admin@rflgd.org with "Attn: Benin Office" in the subject line.

2 Initial Screening

Central administration reviews your request for relevance and urgency within 24 hours.

3 Local Referral

Approved requests are referred to the Cotonou team for direct follow-up within 3-5 days.

BANJUL REGIONAL HUB

Contact RFLD Gambia Office

Our Banjul hub coordinates partnerships and regional advocacy. For inquiries, please contact our central support team for redirection.

Central Contact Email

Main entry point for Gambia inquiries

admin@rflgd.org

Response Time: 3-5 Business Days for Referrals

Contact Procedure

1. **Send Inquiry**
   Email admin@rflgd.org with the subject line "Attention: Gambia Office".
2. **Central Processing**
   Our central team reviews your request to ensure it reaches the correct department in Banjul.
3. **Referral & Response**
   Expect a referral confirmation or direct response from the Gambia team within 3-5 business days.

RESOURCES & SUPPORT

Women's Action Fund (WAFF)

Rapid Response Sub-Granting

Immediate financial assistance mechanism designed for urgent security needs and advocacy interventions.

Supports WHRDs & Grassroots

Direct funding reaches frontline defenders and community organizations often excluded from traditional aid.

Applications Via Published Calls

Funding cycles operate through specific calls for proposals; subscribe to RFLD updates for announcements.

Direct Funding

Empowering local solutions through rapid, flexible grants.

WAFF

WOMEN'S ACTION FUND

RFLD RESOURCES

RFLD Data Center Resources

Country Legal Landscape Intelligence

Comprehensive, up-to-date analysis of cyber laws, gaps, and enforcement trends across 55 African countries.

Evidence for Legislative Advocacy

Verifiable data and statistics to support policy reform campaigns and government engagement strategies.

Digital Safety Compendium Access

A specialized repository of tools, guides, and case studies focused on technology-facilitated gender-based violence.

Actionable Intelligence

FOR SAFER DIGITAL SPACES

RFLD SUPPORT & RESOURCES

Pan-African Network: 156,000 Leaders

Leaders Translate Data Into Change

Our vast network of trained leaders leverages data-driven insights to advocate for policy reforms and societal transformation.

Community-Led Protection & Response

Grassroots defenders lead local protection initiatives, ensuring culturally relevant and rapid responses to digital threats.

Cross-Country Solidarity Activated

A powerful solidarity mechanism mobilizes support across borders, amplifying voices and providing refuge when needed.

156K+

ACTIVE LEADERS

ACTION PLAN

Immediate Steps During Online Attack

Document, De-escalate, Secure Accounts

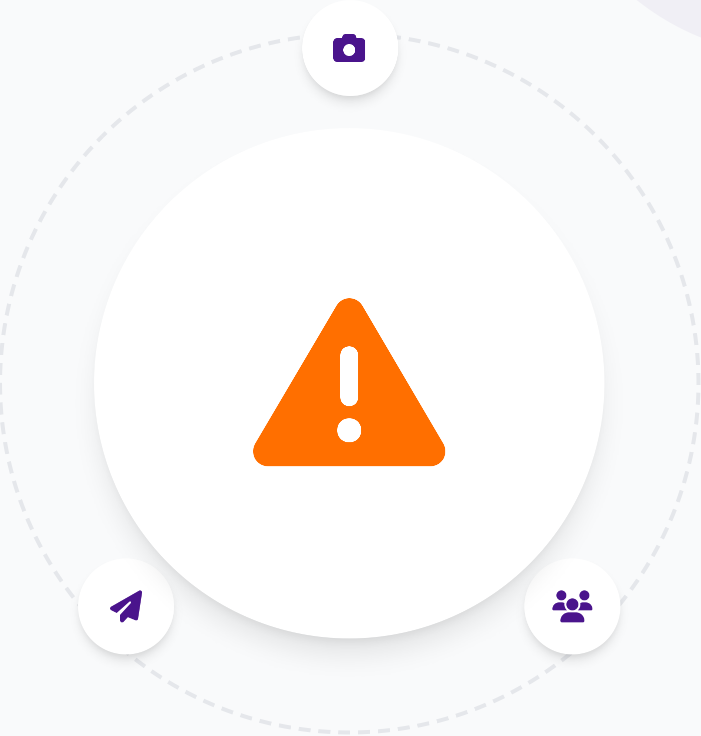
Immediately screenshot evidence, avoid engaging directly with attackers, and enable two-factor authentication on all accounts.

Notify Trusted Network Immediately

Alert close allies, colleagues, and family members to monitor the situation and provide emotional and logistical support.

Report to Platforms Without Delay

Use platform reporting tools for harassment, impersonation, or threats, citing specific policy violations clearly.



First Response

SECURE & REPORT

ACTION PLAN

Safety Planning Checklist

Proactive preparation reduces panic during attacks. Use this checklist to build resilience before a crisis occurs.

Share this plan with your trusted network.

PRIORITY ACTIONS

Update Risk Assessment

Regularly evaluate your digital footprint and identify potential triggers or vulnerabilities before they are exploited.

Secure Address & Records

Remove home addresses from public registries and secure sensitive physical records. Use a P.O. box for public mail.

Crisis Contacts & Backups

Establish offline backup communication channels and maintain a printed list of emergency legal and tech support contacts.

TAKING ACTION

Building Support Networks

Allies, Mentors, Peer Responders

Mobilize trusted allies and mentors to provide immediate emotional support and strategic advice during attacks.

Legal, Psychosocial, Technical Support

Access specialized assistance including legal defense, trauma counseling, and digital security expertise.

Community Moderation Volunteers

Coordinate volunteers to help monitor comments, document abuse, and report violations to platforms effectively.

Stronger

TOGETHER

TAKING ACTION

Community Solidarity Strategies

Amplify Verified Statements

Counter disinformation by widely sharing and promoting the target's official verified narrative and factual rebuttals.

Mass-Report Abusers Collectively

Coordinate community action to report abusive accounts simultaneously, triggering faster platform moderation responses.

Publicly Condemn Gendered Abuse

Organizations and allies must issue joint statements denouncing targeted campaigns to shift public narrative and show support.

Strength in Numbers

United Action Protects All

TAKING ACTION

Advocacy for Law Reform

Promote Survivor-Centered Legislation

Advocate for laws that prioritize survivor safety, streamline reporting processes, and provide clear legal remedies.

Train Police and Prosecutors

Build capacity within justice systems to recognize digital violence, handle digital evidence, and prosecute effectively.

Platform Accountability Mechanisms

Demand transparency and swift action from social media platforms in removing harmful content and banning abusers.

Policy

CHANGE & IMPACT

SYSTEMIC CHANGE

Legislative Victories: Transforming Laws

23 Laws Reformed

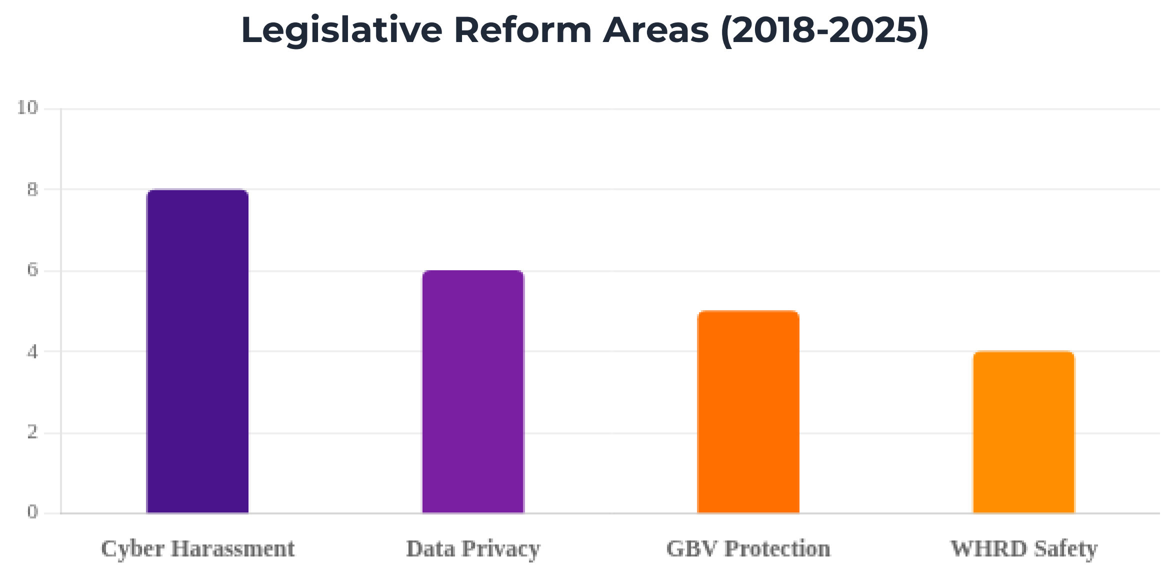
Continent-Wide Impact

Key legislative reforms secured across Africa, directly improving protections for women and digital rights.

12+ Governments

Evidence-Driven Engagement

African governments officially citing RFLD data to shape national gender and digital safety policies.



55
COUNTRIES REACHED

8
MODEL LAWS REPLICATED

Source: RFLD Annual Impact Report 2025, Legislative Tracking Matrix.

TAKING ACTION

Mental Health and Self-Care

Schedule Rest and Decompression

Prioritize offline breaks and recovery time to mitigate the psychological toll of digital attacks.

Reduce Exposure and Curate Feeds

Temporarily mute notifications, block abusive accounts, and limit screen time to protect mental wellbeing.

Access Trauma-Informed Counseling

Seek professional psychosocial support specialized in digital violence to process trauma and build resilience.

You Matter

SELF-CARE IS RESISTANCE

TAKING ACTION

Psychosocial Support Resources & Networks

Confidential Counseling Referrals

Access to vetted, trauma-informed therapists specializing in digital violence impact and recovery.

Peer Support Group Facilitation

Structured safe spaces for survivors to share experiences and build collective resilience strategies.

Emergency Mental Health Lines

24/7 crisis intervention services available regionally for immediate psychological stabilization.

You Are Not Alone

Psychosocial support is a critical component of digital security and holistic protection.

WEST AFRICA

Senegal: Land Rights Reform

A transformative advocacy campaign leveraging data to secure inheritance and ownership rights for women.

Direct Impact

Over 10,000 women secured land titles following legislative changes driven by RFLD's data advocacy.

01

Data-Informed Strategy

RFLD identified that only 12% of women owned land, using this critical data to engage parliamentarians.

●

Legislative Reform

Evidence-based advocacy led to successful inheritance law reform, removing discriminatory barriers to ownership.

●

Community Empowerment

Empowered local women to claim their rights, ensuring sustained monitoring and implementation of new laws.

WEST AFRICA

Benin: Maternal Health Campaign

A data-driven advocacy initiative leveraging localized statistics to secure government funding for essential health services.

Community Impact

Secured funding for new clinics now serving thousands of women annually through evidence-based budget allocation.

01

Rights-Based Budgeting

Utilized RFLD's data to demonstrate gaps in maternal healthcare funding and the direct impact on women's lives.

Data-Driven Advocacy

Local leaders presented irrefutable statistics to municipal councils, linking health outcomes directly to budget lines.

Clinics Funded & Operational

Successfully secured sustained public funding for new clinics, establishing a model for rights-based budgeting.

WEST AFRICA

Ghana: WHRD Protection

A comprehensive protection strategy safeguarding women human rights defenders from targeted digital and physical threats.

Protection Impact

RFLD's emergency response mechanisms successfully intervened to protect high-risk defenders during critical threat periods.

01

Emergency Response

Deployed rapid emergency assistance and safe relocation protocols for defenders facing imminent online-to-offline threats.

Digital Safety Capacity

Significantly increased technical capacity through specialized digital security training, equipping defenders with preventative tools.

Police Cooperation

Established improved protocols and direct cooperation channels with police units to handle digital violence reports effectively.

KENYA

Legal Victory: Cyberbullying Case

A precedent-setting ruling that affirmed online harassment is a punishable criminal offense under Kenyan law.

Judicial Impact

The ruling set a vital precedent for holding perpetrators of digital violence accountable in East African courts.

01

Harassment Recognized

The court formally recognized that persistent online abuse constitutes criminal harassment, rejecting "free speech" defenses.

Act Applied Effectively

Prosecutors successfully applied Section 27 of the Computer Misuse and Cybercrimes Act to charge and convict the offender.

Precedent for Action

Established a clear legal pathway for swift judicial intervention in future cases of technology-facilitated gender-based violence.

WEST AFRICA

Nigeria: Platform Accountability

A precedent-setting case establishing platform liability and enforcing takedowns of harmful digital content.

Judicial Precedent

Federal High Court ruling mandates swift platform action on verified harassment reports to protect digital rights.

01

Court-Ordered Takedown

Secured a binding court order compelling social media platforms to remove non-consensual images and abusive content.

Service Provider Cooperation

Enforced compliance from internet service providers to preserve data logs and identify anonymous perpetrators.

Legal Aid Support

Provided pro bono legal representation and technical evidence support through RFLD's partner network.

PAN-AFRICAN NETWORK

Regional Solidarity

Leveraging our 55-country network to provide seamless protection, advocacy, and support across borders when national systems fail.

Network Power

156,000 leaders activate simultaneously to protect defenders, creating a safety net that transcends national borders.

Coordinated Responses

Activating rapid response networks across multiple network countries to launch unified defense campaigns for targeted members.

Resource Sharing & Relocation

Facilitating urgent safe passage and relocation to safe houses in neighboring countries, sharing legal and financial resources.

Regional Documentation

Compiling cross-border evidence of digital repression to submit robust reports to regional bodies like ACHPR and ECOWAS.

CONCLUSION

Building Digital Resilience Together

Collective Care and Coordination Models

Shifting from individual burden to shared responsibility through community-led protection networks and mutual aid.

Evidence, Advocacy, Accountability Pillars

Using documented data to demand legal reforms and holding tech platforms and perpetrators accountable.

Sustained, Intersectional Approaches Required

Developing long-term strategies that address diverse needs across gender, region, and identity for lasting safety.

Solidarity

IS OUR PROTECTION

EMPOWERMENT

Your Rights, Your Power

Know frameworks protecting your rights

Understanding international and national laws empowers you to identify violations and demand protection.

Assert, document, seek timely remedies

Take action by meticulously documenting abuse and using reporting mechanisms to hold perpetrators accountable.

Remember you are not alone

You are part of a vast network of defenders and allies ready to support your safety and advocacy.

Stand

TOGETHER

GET INVOLVED

Join RFLD's Pan-African Movement

Partner, Volunteer, Co-Create Solutions

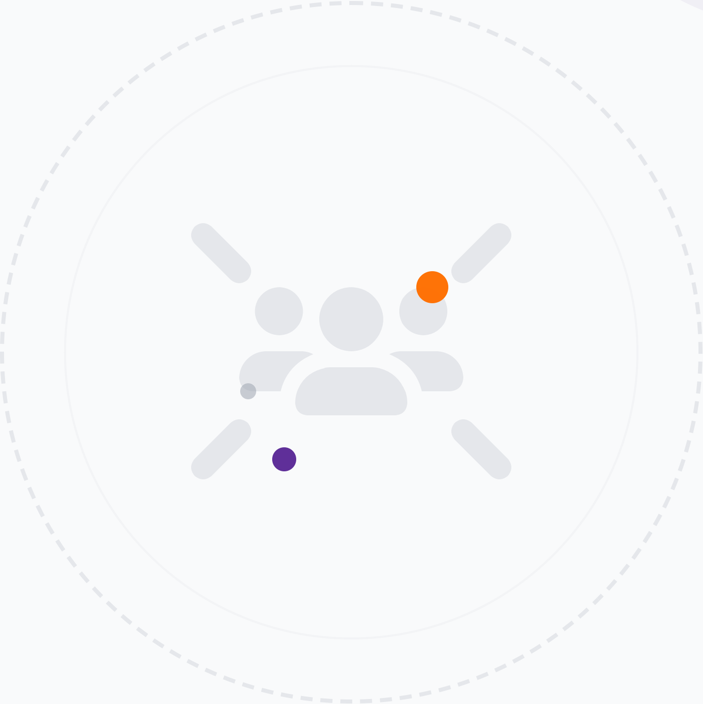
Collaborate with our diverse network of 156,000 leaders to design and implement community-led interventions.

Amplify Feminist Digital Safety Initiatives

Use your platform to share this toolkit, raise awareness, and challenge the normalization of online gender-based violence.

Support Funding and Advocacy Efforts

Contribute resources to sustain protection programs, legal aid funds, and legislative advocacy campaigns across Africa.



Take Action

BECOME A MEMBER

GET IN TOUCH

Reach Out for Support & Partnership

Whether you need assistance, want to partner, or have inquiries, our team is ready to connect with you.

General Inquiries & Support

Central contact for all requests

admin@rflgd.org

Response Time: Within 3-5 Business Days

Communication Guidelines

1. **Clear Subject Line**
   Use specific subjects like "Partnership Inquiry - [Org Name]" or "Support Request - [Topic]" to ensure routing.

2. **Provide Context**
   Briefly describe your inquiry, relevant background, and specific needs to help us respond effectively.

3. **Follow-Up**
   If you don't hear back within 5 business days, please send a polite follow-up reminder.

CONCLUSION

Thank You:
Safe Digital Spaces for All

Share This Toolkit Widely and Freely

Distribute this resource to networks, colleagues, and communities to amplify legal protection knowledge.

Train Colleagues and Community Members

Use these materials to facilitate workshops and build collective digital safety capacity across organizations.

Together, We End Digital Violence

By documenting, reporting, and supporting each other, we reclaim online spaces for feminist expression.

#RFLDLegalToolkit

Empowering Digital Rights

www.rflgd.org