DRF COMMENTS ON THE NATIONAL STRATEGY TO ADDRESS TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE 2025–2030

Digital Rights Foundation (DRF) welcomes the development of the National Strategy to Address Technology-Facilitated Gender-Based Violence (TFGBV) 2025–2030 as Pakistan's first comprehensive attempt to articulate a coordinated national framework for addressing the growing crisis of online and technology-facilitated abuse. The Ministry of Human Rights' recognition of the urgency and scale of TFGBV is timely, particularly given the rapid technological shifts shaping digital violence, including artificial intelligence, deepfake technologies, synthetic media, and platform-driven harms.

DRF acknowledges that the Ministry of Human Rights engaged civil society organisations during consultations, and we appreciate the openness to external feedback. However, the strategy in its current form does not meaningfully integrate civil society experience, infrastructure, or expertise into the implementation architecture. Consultations were held, but the strategy does not reflect a multi-stakeholder governance model, and civil society, particularly frontline organisations such as DRF, is not embedded as an equal partner in prevention, protection, prosecution, response, or monitoring processes.

This remains a critical omission, especially given that organisations like DRF have been operating TFGBV helplines, providing survivor support, conducting capacity building, training law enforcement, and documenting systemic failures for more than a decade. The absence of civil society from formal governance and coordination structures limits the strategy's effectiveness and undermines its survivor-centred intent.

In addition, DRF notes that while the strategy is visionary in scope and ambitious in its goals, many proposed mechanisms are not realistically aligned with current institutional capacity, legal frameworks, resource availability, or technological limitations. Without practical, phased, and actionable pathways, several commitments risk remaining aspirational rather than implementable. A national strategy of this magnitude must balance ambition with feasibility, particularly given the historic challenges of implementation across federal and provincial institutions.

This document therefore offers detailed analysis of the strategy's strengths, gaps, risks, and opportunities, followed by practical recommendations grounded in international human rights standards, global regulatory trends, and over a decade of DRF's experience working directly with survivors of technology-facilitated violence in Pakistan.

Overarching Concerns and Structural Gaps

1. Lack of Practical and Phased Implementation Measures

While the strategy articulates an expansive vision, it does not adequately address the practical constraints that have historically undermined digital rights and gender-based violence frameworks in Pakistan. Important proposals, such as establishing SDPO-level cybercrime units, creating new regulatory bodies, implementing 24-hour takedown mandates, developing real-time survivor tracking systems, and deploying AI-assisted case management, require:

- significant operational budgets
- legislative reform across multiple ministries
- long-term political consistency
- specialized technical skill sets
- interdepartmental coordination mechanisms
- functional data protection rules that currently do not exist
- cooperation from global technology companies

In the absence of these prerequisites, these proposals may be difficult to operationalize in the short or medium term.

DRF believes a more realistic approach would involve phased implementation, prioritization of high-impact interventions, capacity building, and pilot testing before nationwide rollout. A strategy that is overly ambitious without acknowledging capacity constraints risks stagnation and undermines trust among stakeholders and survivors.

2. Consultation Without Structural Inclusion of Civil Society

Although civil society was consulted during the drafting process, the strategy does not embed CSOs in the governance architecture. The National TFGBV Coordination Cell, inter-ministerial working groups, monitoring mechanisms, implementation structures, and platform accountability processes are entirely state-centric. CSOs appear as optional partners rather than essential actors.

Globally, digital safety and TFGBV strategies rely heavily on survivor-led, women-led, and digital rights organisations for their operational success. The EU Digital Services Act, Australia's eSafety framework, Canada's online harms model, and regional feminist digital justice networks embed civil society directly into the governance structure. Pakistan's strategy does not do so and risks producing a bureaucratic system disconnected from real survivor pathways.

DRF strongly recommends formal, statutory inclusion of civil society at every stage of implementation, monitoring, coordination, and accountability.

3. Risk of Chilling Effects on Survivors

A central concern is the lack of explicit safeguards ensuring that the strategy encourages survivors to seek help rather than deterring them. Survivors already avoid reporting technology-facilitated abuse due to fear of moral policing, privacy breaches, insensitive handling, exposure to male-dominated offices, and mistrust in state institutions. The strategy does not articulate clear protections for survivor privacy, dignity, consent, anonymity, data handling, or independent oversight.

A national TFGBV strategy must clearly state how the Ministry will prevent institutional retraumatization and ensure that reporting is accessible, safe, confidential, and survivor-affirming.

4. Lack of Rights-Based Safeguards and International Standards

The strategy does not sufficiently integrate:

- CEDAW General Recommendation 35
- UN Special Rapporteur guidance on digital VAWG
- UN High Commissioner for Human Rights standards on digital regulation
- Santa Clara Principles on transparency and accountability
- Global best practices on due process and content governance

Without clear safeguards, there is a risk that certain provisions, especially around content removal, data requests, and platform penalties, may be misused.

Practical Solutions Rather Than Aspirational Measures

Across multiple sections, the strategy proposes mechanisms that, while conceptually sound, require more realistic, step-by-step implementation pathways. DRF proposes the following guiding principles for practicality:

1. Focus on reforms that can be implemented within existing institutional structures.
2. Prioritize training, capacity building, and resources for institutions that already exist rather than creating new ones.
3. Pilot digital systems (case management, takedown coordination) in major cities before nationwide implementation.
4. Establish phased timelines for expansion based on demonstrated performance.
5. Ensure new mandates are legally, technically, and financially feasible before adoption.

6. Embed independent oversight, civil society monitoring, and transparency in all stages.

7. Align content removal and platform accountability mechanisms with international due process standards.

These principles will be elaborated in the relevant sections of this critique.

Legal and Conceptual Gaps in the Strategy

The strategy presents an extensive review of Pakistan's legislative frameworks, particularly the Prevention of Electronic Crimes Act (PECA) and the proposed Social Media Protection and Regulatory Authority (SMRA). However, the document does not sufficiently acknowledge the widely documented limitations, political misuse, and institutional constraints embedded within these laws. PECA has historically been deployed to silence journalists, activists, and dissenting voices, and has rarely served as an effective instrument for survivors of technology-facilitated violence.

This disconnect between legislative intention and real-world outcomes requires open acknowledgement. Without addressing how PECA's structural problems will be resolved, the strategy's reliance on its provisions appears overly optimistic.

Additionally, the absence of a comprehensive data protection law undermines all proposed measures involving data collection, evidence handling, platform cooperation, cross-border information sharing, and AI-supported systems. Any TFGBV strategy that expands state access to sensitive data without a rights-respecting data protection framework risks causing further harm to survivors and compromising public trust.

Gaps in Legislative Clarity

The strategy lacks clarity on several legal concepts and procedural steps required for coherent implementation. This includes:

1. Definitions of TFGBV-related offences, including viral harassment, non-consensual image-based abuse, synthetic content, and credible threats.

2. Clear thresholds for what constitutes a high-risk case.

3. Procedural standards for data requests, takedown orders, and platform compliance while following **three part tests including legitimate aim, legality and necessity and proportionality principles.**

4. Safeguards to ensure that content removal powers are not misused for censorship, check above three part test.

5. Judicial oversight mechanisms to ensure legality and due process.

6. Appeal and review structures for victims and respondents.

DRF stresses the need for clarity and precision in legislative definitions and procedures. Vague terminology in digital regulation is prone to misuse and can disproportionately affect human rights defenders, journalists, and marginalised communities, the way we have witnessed over the years in PECA's implementation.

Ambition Without Legal Feasibility

Several proposed reforms require significant amendments to existing laws, including PECA, the Telegraph Act, and Pakistan's constitutional framework for fundamental rights. The strategy does not detail how these legal changes will be achieved, particularly in a context where legislative reform is often delayed and contested.

Given these realities, DRF recommends adopting a phased legal roadmap that begins with achievable administrative reforms, clear guidance for law enforcement, and evidence-based amendments that can realistically pass through legislative processes.

Analysis of the PECA 2025 Amendment

While PECA 2025 aims to expand regulatory powers and streamline content removal, it has been widely criticised by civil society, digital rights experts, media organisations, and frontline defenders for being overly broad, politically influenced, and potentially restrictive of freedom of

expression. The strategy's reliance on PECA 2025 therefore raises serious concerns regarding both its legitimacy and its capacity to serve survivors of technology-facilitated gender-based violence.

In addition to structural issues, it must be acknowledged that PECA has a documented history of **misuse**, including against journalists, human rights defenders, political dissenters, and even **survivors of harassment who attempted to speak out under the MeToo movement**. Survivors reporting digital abuse have at times been threatened with counter-cases under PECA provisions, creating a chilling effect and discouraging women from seeking help. This historical misuse must be openly recognised, especially within a TFGBV strategy whose primary goal is to build trust and safety for survivors.

Key Concerns

1. The proposed Social Media Protection and Regulatory Authority creates another centralised regulator without ensuring independence, transparency, or judicial oversight.

2. The strategy does not address risks of selective enforcement, political misuse, or regulatory overreach, all of which have occurred repeatedly under PECA since 2016.

3. The complaint-handling and appeals processes remain unclear, increasing the likelihood that survivors will be passed between multiple institutions without a resolution.

4. The 24-hour content removal mandate lacks alignment with due process, international human rights standards, and necessary procedural safeguards.

5. The amendment remains contentious within civil society and media communities, which undermines the foundation upon which the strategy relies.

Need for Oversight That Has Real Authority

Given PECA's history of misuse and the potential for further overreach, the strategy must include **robust oversight mechanisms** that go beyond internal government checks. This should include:

- **Parliamentary oversight** with mandatory annual reporting on PECA enforcement
- **Judicial oversight** for content removal, data requests, and platform penalties
- **Independent oversight bodies** with civil society representation and the authority to audit, review, and challenge misuse

These oversight structures must have real authority, clear enforcement powers, and the ability to hold state institutions accountable for violations or selective implementation. Without these safeguards, reliance on PECA for TFGBV protection risks replicating the very harms the strategy seeks to prevent.

DRF Recommendation

Given the contentious nature of PECA 2025, and the pattern of misuse of PECA more broadly, the strategy should not rely solely on this amendment. Instead, it should adopt a layered and rights-respecting approach that:

1. Strengthens institutional capacity within NCCIA and provincial police to respond sensitively and efficiently to TFGBV cases.
2. Clearly defines TFGBV-related legal provisions to eliminate ambiguity and prevent misuse.
3. Introduces strong survivor-centric protections within all evidence-handling protocols.
4. Embeds international human rights safeguards consistent with CEDAW, ICCPR, and UN Special Rapporteur guidance.
5. Includes civil society as formal partners in reviewing, auditing, and monitoring the implementation of PECA reforms.

6. Ensures parliamentary, judicial, and independent oversight mechanisms that have real authority to correct misuse, protect survivors, and strengthen public trust.

Strengthening this section will ensure the strategy accurately reflects Pakistan's historical context, survivor realities, and international standards for safe and rights-respecting digital regulation.

SMRA Design, Limitations, and Risks

The strategy envisions SMRA as a central solution for platform accountability, content removal, and regulatory oversight. However, several structural risks remain unaddressed.

Unclear Jurisdiction

The division of responsibilities between SMRA, the Social Media Complaint Council, and the Tribunal is not clearly explained. This ambiguity risks confusion and delays, particularly for survivors seeking urgent protection. The strategy should clearly outline which body handles what type of complaint and how cases transition between them.

Risk of Over-Centralisation

Concentrating content regulation powers within a single authority without transparency or independent oversight can increase the risk of censorship or selective enforcement. International experience shows that such authorities must operate within strict human rights frameworks to avoid abuse.

Lack of Feasible Enforcement Pathways

The strategy does not articulate how SMRA will enforce compliance against global platforms that do not maintain physical presence or legal incorporation in Pakistan. Local blocking is a limited tool, often harming users without effectively compelling platform compliance.

Recommendations for Practical and Rights-Respecting SMRA Design

1. Establish independent oversight committees, including CSOs and digital rights experts.
2. Create clear, narrow, rights-based definitions for content subject to takedown.
3. Require all takedown and data requests to meet legality, necessity, and proportionality tests.
4. Publish quarterly transparency reports of actions taken, requests issued, and outcomes.
5. Ensure that data preservation procedures exist to prevent loss of evidence before content removal.

Gaps in Evidence Collection, SOPs, and Data Protection

The strategy acknowledges the need for SOPs on evidence handling but does not provide substantive detail on how these will be developed or enforced. This is a crucial omission.

Survivor Data Protection Must Be Central

A TFGBV strategy cannot succeed without strong data protection guarantees. Survivors already hesitate to report technology-facilitated violence due to fears of privacy breaches, leaks, and misuse of personal information. Without:

- encryption requirements
- limited data retention policies
- informed consent protocols
- anonymity options
- independent audits
- secure cross-agency transfer systems

- penalties for breaches

survivor trust cannot be built.

Current Data Handling Practices Are Not Safe

NCCIA's existing data systems have repeatedly faced:

- manual data storage
- weak digital security
- insufficient equipment
- dependence on WhatsApp-based communication
- lack of secure evidence lockers
- inconsistent chain-of-custody procedures

The strategy overlooks these practical realities.

Recommendations

1. Create detailed SOPs for collection, preservation, transfer, and deletion of digital evidence.
2. Require all agencies to use encrypted devices, secure server systems, and protected communication channels.
3. Establish survivor consent protocols at every stage.
4. Ensure data minimization for all TFGBV cases.

5. Develop digital evidence handling manuals aligned with international cybercrime guidelines.

INSTITUTIONAL GAPS, PLATFORM ACCOUNTABILITY, AI RISKS, SURVIVOR PROTECTION, AND THE CRITICAL NEED TO STRENGTHEN ENCRYPTION

The strategy identifies multiple institutions responsible for responding to technology-facilitated gender-based violence, including NCCIA, SMRA, provincial police bodies, prosecutors, and courts. However, the document does not clearly explain how these institutions will coordinate, share information, avoid duplication, or ensure survivor-friendly procedures. In practice, survivors often find themselves moving between different agencies without clarity or support, resulting in retraumatization and delayed justice.

Need for a Coherent Interagency Workflow

The strategy proposes new layers of institutional responsibility without simplifying existing ones. Without a clear, unified reporting pathway, the burden continues to fall on survivors to navigate the system. International best practice encourages creating a single point of contact for survivors, backed by interoperable systems between relevant agencies.

Civil Society Must Be a Formal Partner in Coordination

Civil society organisations, especially those like DRF that operate helplines, digital security clinics, and direct casework, possess unique insights into survivor pathways. This expertise is essential for designing integrated institutional workflows. The strategy currently does not reflect this learning and therefore risks producing systems that remain bureaucratic and survivor-unfriendly.

DRF recommends creating a formal role for civil society across all coordination working groups, technical committees, and implementation teams so that lived survivor experience informs operational design.

The Need to Strengthen Encryption Rather Than Weaken It

A critical element missing from the strategy is a clear commitment to **preserving and strengthening end-to-end encryption**, which is globally recognised as a foundational safeguard for vulnerable populations, including TFGBV survivors.

Survivors of harassment, stalking, extortion, and image-based abuse rely heavily on secure digital communication to:

communicate safely with support networks
seek legal or psychosocial guidance
share evidence securely
avoid surveillance by abusers or hostile family members
maintain privacy in coercive, high-risk environments

Weakening encryption in the name of safety often has the unintended effect of putting survivors at greater risk.

International Standards

UN Special Rapporteurs, the OHCHR, and global human rights bodies consistently affirm that:

strong encryption protects women and marginalised communities
backdoors or access mandates disproportionately harm survivors
secure communication is essential to privacy, consent, agency, and autonomy

The strategy currently suggests measures that, if interpreted incorrectly, could justify weakening encryption in the name of enhanced detection or data access. This would undermine survivor safety and contradict international human rights standards.

DRF's Recommendation

Pakistan's TFGBV strategy must **explicitly commit to protecting and strengthening encryption** by incorporating the following principles:

Online safety must not come at the cost of weakening encryption
Platforms should not be compelled to introduce backdoors or blanket access mandates
Secure channels must be protected for survivors to reach help safely

Lawful access should be pursued only through narrow, judicially authorised, case-specific processes
Any regulatory measures must comply with international standards on privacy and free expression
Strong encryption is a prerequisite for survivor-centred digital safety

This ensures the strategy does not unintentionally enable surveillance, retaliation, or further violence.

Platform Accountability: Limitations and Necessary Reforms

The strategy's intention to expand platform accountability is important, but the proposed mechanisms remain vague, overly ambitious, or legally unenforceable under current conditions. Expectations must remain grounded in platform policy realities and Pakistan's current regulatory limitations.

Lack of Realistic Enforcement Pathways

Platforms vary greatly in scale, operational structure, moderation capacity, and language resources. For example:

Large platforms such as Meta, YouTube, and TikTok have formal moderation processes but insufficient Urdu or regional language expertise
Smaller platforms often lack local compliance teams entirely

Applying a single compliance standard to all platforms is neither realistic nor enforceable. Without differentiation, accountability models risk collapsing in implementation.

Risk of Overreach Without Safeguards

Enforcement measures such as fines, warnings, and performance scoring require:

judicial oversight
due process
transparency
clear criteria

legal grounding
independent audits

Without these safeguards, the system risks misuse, overreach, or politically motivated enforcement, which disproportionately harms women, journalists, and human rights defenders.

Need for Transparency and Public Reporting

Platforms operating in Pakistan must publish annual public transparency reports on:

response times to TFGBV cases
compliance with government requests
language-specific moderation
cooperation levels with law enforcement
appeal outcomes

These reports must remain public to allow civil society oversight and survivor trust-building.

Civil Society Participation in Platform Accountability

Globally, civil society plays an essential role in contextual analysis, community reporting, identifying emerging harms, and shaping platform policies. DRF recommends formal representation of CSOs in all platform accountability structures, including joint review mechanisms.

Concerns Around Automated Moderation and Misinformation Provisions

The strategy proposes automated systems to detect non-consensual intimate images, synthetic content, and misinformation. While technological tools can assist, automated moderation has significant limitations, particularly in Pakistan's linguistic landscape.

Limitations of Automated Detection

Automated systems struggle with:

Urdu and regional languages
context-dependent harassment
distinguishing satire, critique, or political speech
identifying synthetic media without watermarking
detecting nuanced TFGBV indicators

Overreliance risks both under-enforcement and over-enforcement, harming survivors and legitimate expression.

The Ambiguity of "Misinformation"

"Misinformation" is a politically charged term worldwide. Without narrow and precise definitions, its inclusion in TFGBV regulation risks misuse.

Any regulation referencing misinformation must be:

aligned with necessity and proportionality
subject to judicial oversight
narrowly tailored
bound by human rights standards

AI-Assisted Case Classification: Risks and Practical Alternatives

The strategy proposes AI-assisted case classification to prioritise high-risk complaints. DRF cautions strongly against deploying automated classification systems for sensitive TFGBV cases.

AI Cannot Capture Pakistan's Social and Cultural Nuance

TFGBV cases often involve:

familial coercion
honour-based threats
intersecting vulnerabilities
community-level dynamics

gendered psychological harm
sociocultural context

AI cannot adequately evaluate these realities and risks misclassifying urgent cases.

Data Protection Risks

AI models require large datasets of sensitive survivor information. In the absence of a privacy law and secure infrastructure, this introduces dangerous risks of:

data breaches
secondary victimisation
permanent retention of sensitive content
misuse by hostile actors

Practical, Implementable Alternative

DRF recommends:

human-led case assessment by trained TFGBV officers
standardised prioritisation checklists
mandatory trauma-informed training
internal monitoring of timelines
clear escalation protocols

These alternatives are practical, achievable, and rights respecting.

Survivor Protection and Law Enforcement Capacity

Female Officers Alone Are Not Enough

While female officers can improve comfort for survivors, gender alone cannot substitute for:

trauma-informed training
intersectional understanding
competent digital evidence handling
survivor-sensitive communication
clear internal accountability

Female officers in Pakistan often lack autonomy, resources, and training. Without systemic reform, simply increasing female staffing will not improve outcomes.

Training Must Be Continuous

Effective TFGBV response requires systems-level training on:

trauma-informed interviewing
gender-sensitive protocols
local sociocultural dynamics
privacy and consent
secure evidence handling

Training should be institutionalised, not ad hoc.

Civil Society's Essential Role in Survivor Support

CSOs maintain deep community trust and are often a survivor's first point of contact. Formalising partnerships would:

improve referral pathways
increase reporting
provide psychosocial and digital security support
enhance survivor empowerment
build institutional trust
ensure policy reflects lived experience

The strategy must integrate these roles into its formal architecture.

GOVERNANCE, MONITORING, INTERNATIONAL COOPERATION, PRACTICALITY, FINAL RECOMMENDATIONS

Governance and Coordination

While the strategy proposes the establishment of a National TFGBV Coordination Cell and multiple inter-ministerial working groups, the governance structure remains heavily government-centric and risks reproducing the same bureaucratic bottlenecks that survivors have historically struggled with.

The framework acknowledges civil society but does not embed CSOs as equal partners in planning, implementation, or oversight. Notably, Pakistan's most consistent and technically specialised work on TFGBV has come from civil society organisations such as DRF, which operate frontline helplines, conduct digital forensics support, advise survivors, and maintain longitudinal data sets. Despite this, the strategy does not create a formal mechanism for CSOs to act as co-implementers, co-monitors, or co-reviewers of TFGBV policy.

DRF strongly recommends the formal inclusion of civil society in all governance structures to ensure transparency, accountability, and survivor-sensitive policymaking. This is particularly important in a context where survivors often distrust state institutions and seek first contact with civil society support systems.

Without formal, structured, and sustained CSO inclusion, the multistakeholder character of the strategy remains superficial and the implementation risks becoming overly bureaucratic and detached from on-ground realities.

DRF Recommendations

Civil society should be formally integrated into:
- National TFGBV Coordination Cell advisory role
- Inter-ministerial working groups
- Monitoring and review mechanisms

Platform accountability reviews

Working groups on curriculum development, community interventions, and evidence-handling protocols

This integration would align Pakistan's framework with international digital governance best practices, including those used in the EU, and Australia's Safety Commissioner model.

Monitoring and Evaluation (M&E)

The strategy sets out ambitious performance indicators such as increasing prosecution rates from 0.6 percent to 15 percent and reducing cases with no meaningful outcome from 65 percent to under 20 percent. While these ambitions demonstrate commitment, they lack practical pathways to achieve them.

Given the severe institutional capacity constraints, these targets risk remaining aspirational unless accompanied by realistic budgeting, staffing, and infrastructure development. Furthermore, the strategy does not sufficiently explain who will monitor these indicators, how data will be collected, or how transparency will be ensured.

DRF notes that without independent oversight, public transparency, and CSO inclusion, monitoring risks becoming an administrative exercise rather than a meaningful mechanism for accountability.

DRF Recommendations

1. Ensure that gender-disaggregated TFGBV data collected by NCCIA, police, SMRA or PTA, and courts is published regularly in aggregated and anonymized form.

2. Mandate annual independent audits of TFGBV responses led jointly by civil society and government.

3. Publish biannual platform transparency reports on content removal, data requests, and responsiveness to TFGBV cases.

4. Embed judicial and parliamentary oversight over critical enforcement mechanisms such as platform penalties, data access, and SMRA powers.

5. Operationalise survivor feedback mechanisms that allow anonymous, secure reporting of gaps or misconduct.

International Cooperation

The strategy calls for cross-border cooperation, mutual legal assistance agreements, and a regional coalition for platform accountability. While these are important long-term goals, they remain extremely ambitious given Pakistan's current diplomatic, legal, and capacity constraints.

The strategy does not outline practical steps for achieving these goals or consider the significant divergence in legal frameworks, capacities, and geopolitical interests across South Asia and the MENA region.

DRF stresses the need for a pragmatic, phased approach.

DRF Recommendations

Focus first on achievable bilateral arrangements with countries where major platforms hold data centres such as Ireland, Singapore, and the United States
Secure technical assistance from UN Women, UNDP, UNODC, and the Special Rapporteur on Violence Against Women and Girls on cross-border TFGBV cases
Develop a cross-agency protocol for international MLAT processing to reduce delays
Avoid premature commitments to regional coalitions without feasibility studies and rights safeguards

Practicality and Implementation Challenges

A recurring concern across the entire strategy is the risk of over-ambition without operational feasibility. The document introduces new authorities, specialised units, complex AI systems,

platform enforcement models, data protocols, and regional coalitions without clear budgeting, capacity assessments, or implementation sequencing.

Historically, Pakistan has struggled to implement far simpler reforms in cybercrime investigation, digital evidence handling, and survivor support. Without realistic grounding, the risk is that the strategy becomes a visionary document that remains on paper rather than transforming the lived experience of survivors.

DRF Core Observations

1. Many proposed structures mirror existing bodies rather than strengthening what already exists.

2. Resource limitations across NCCIA, police, courts, and prosecution make immediate implementation unrealistic.

3. The strategy contains numerous unfunded mandates.

4. Survivors may continue to face the same systemic barriers if institutional reforms remain slow.

5. Focus should remain on strengthening and resourcing existing institutions before creating new ones.

The strategy should adopt a more pragmatic, incremental approach that prioritises:

Enhancing NCCIA capacity
Improving digital evidence handling
Ensuring police and prosecutors receive TFGBV training
Creating genuine survivor-centred grievance mechanisms
Strengthening SMRA only after clear oversight structures are in place
Embedding civil society in implementation at every step

This approach will ensure that commitments translate into real outcomes and do not remain aspirational.

Final Recommendations

To ensure that the National TFGBV Strategy becomes an actionable, survivor-centred, and rights-respecting framework rather than an overly ambitious blueprint, DRF strongly recommends the following revisions:

Fully integrate civil society as equal partners in implementation, monitoring, and platform engagement
Ground platform accountability mechanisms in international human rights law and establish judicial, parliamentary, and independent oversight
Ensure that TFGBV definitions, content removal processes, and emergency protocols are precise, rights-respecting, and rooted in safeguards
Invest in realistic, survivor-centred institutional reforms before creating new structures
Strengthen evidence handling, digital forensic capacities, and trauma-informed procedures across NCCIA and police
Ensure public transparency in data reporting, platform cooperation, and state actions
Embed comprehensive data protection safeguards and accelerate adoption of a rights-respecting data protection law
Adopt a phased implementation model that scales gradually with institutional capacity
Guarantee that the law is encouraged for survivors' use rather than generating chilling effects
Acknowledge PECA's historical misuse and introduce strong checks to prevent repetition

DRF reiterates that survivors' safety, dignity, and access to justice must remain the central focus of Pakistan's national strategy. Any framework addressing TFGBV must reflect not only the urgency of the issue but also the deeply contextual realities and constraints facing institutional systems.

With meaningful reform, inclusive governance, and practical implementation, Pakistan can establish a TFGBV response that is survivor-centred, rights-aligned, and sustainable.