



MINISTRY OF HUMAN RIGHTS  
GOVERNMENT OF PAKISTAN

# NATIONAL STRATEGY TO ADDRESS TECHNOLOGY - FACILITATED GENDER-BASED VIOLENCE (TFGBV)

2026-2030

A coordinated, survivor-centred approach  
to addressing digital violence against women  
and vulnerable communities in Pakistan

NATIONAL STRATEGY  
TO ADDRESS  
TECHNOLOGY - FACILITATED  
GENDER-BASED VIOLENCE  
(TFGBV)

2026-2030

# CONTENTS

ACKNOWLEDGMENTS	3
FOREWORD	4
MESSAGE BY THE SECRETARY	5
MESSAGE BY THE UNDP RESIDENT REPRESENTATIVE	6
VISION	7
MISSION STATEMENT	7
EXECUTIVE SUMMARY	8
KEY OBJECTIVES	9
<b>1. EXPECTED OUTCOMES</b>	<b>11</b>
1. BACKGROUND AND CONTEXT	17
1.1 Spectrum of the Issue	17
1.2 Constitutional Framework	20
<b>2. INTERNATIONAL OBLIGATIONS AND COOPERATION</b>	<b>21</b>
2.1 CEDAW Alignment	21
2.2 Transnational Linkages	21
<b>3. LEGISLATIVE FRAMEWORK</b>	<b>22</b>
3.1 PECA 2016-2025	22
3.2 PECA Amendment 2025 - New Regulatory Framework:	23
<b>4. INSTITUTIONAL FRAMEWORK</b>	<b>25</b>
4.1 National Cyber Crime Investigation Agency (NCCIA)	25
4.2 Platform Accountability Crisis	25
4.3 Regulatory Framework: Pakistan Telecommunication Authority, Social Media Regulatory Authority, Council and Tribunal	26
<b>5. POLICY ALIGNMENT AND INTEGRATION</b>	<b>30</b>
<b>6. STRATEGIC FRAMEWORK: THE PPPR APPROACH</b>	<b>32</b>

6.1 PILLAR 1: PREVENTION	33
6.2 PILLAR 2: PROTECTION	35
6.3 PILLAR 3: PROSECUTION	39
6.4 PILLAR 4: RESPONSE	41
<hr/>	
<b>7. ADDRESSING EMERGING TECHNOLOGY CHALLENGES</b>	<b>46</b>
7.1 AI-Generated Content Crisis	46
7.2 Understanding Perpetrator Behaviour - MMO Framework	47
<hr/>	
<b>8. IMPLEMENTATION FRAMEWORK</b>	<b>49</b>
8.1 Governance Structure	49
8.2 Integrated Support Systems	50
8.3 Implementation Strategy	51
<hr/>	
<b>9. MONITORING AND EVALUATION FRAMEWORK</b>	<b>54</b>
9.1 Performance Indicators and Baseline Metrics	54
<hr/>	
<b>10. INTERSECTIONAL APPROACHES AND VULNERABLE POPULATIONS</b>	<b>55</b>
<hr/>	
<b>11. RISK MANAGEMENT AND MITIGATION STRATEGIES</b>	<b>56</b>
11.1 Implementation Challenges and Mitigation	56
11.2 Monitoring and Course Correction	57
<hr/>	
<b>12. CONCLUSION AND CALL TO ACTION</b>	<b>58</b>

## ACKNOWLEDGMENTS

Developed under the auspices of of the Ministry of Human Rights (MoHR), Government of Pakistan, and in collaboration with the United Nations Development Programme (UNDP) Pakistan, Pakistan's First National Strategy on Technology-Facilitated Gender-Based Violence (TFGBV) reflects a shared commitment to establishing a coordinated, rights-based, and survivor-centred national response to technology-facilitated harm.

The Ministry of Human Rights and UNDP Pakistan express their appreciation to the institutions and partners whose expertise and engagement informed the Strategy's development. The Ministry and UNDP Pakistan also commend the strategic leadership and oversight of the Secretary, Ministry of Human Rights, and the Deputy Resident Representative, UNDP Pakistan, whose direction and stewardship were pivotal in guiding the Strategy's development from consultation through validation. We recognize the contributions of government entities; criminal justice institutions; regulatory and oversight bodies; actors within the technology and digital ecosystem; civil society and survivor-support organizations; academia; and development partners who provided technical inputs during consultations and validation. Their perspectives strengthened the Strategy's relevance, feasibility, and alignment with national priorities.

The Ministry of Human Rights and UNDP Pakistan further note that sustained collaboration among stakeholders will be essential to effective implementation and continued progress on digital safety and gender equality in Pakistan.

**Core Team:**

Amna Baig – Police Service of Pakistan

Muhammad Arif – Director (IC), Ministry of Human Rights

Nadia Tariq Ali – Head of the Gender Team, UNDP

## FOREWORD



It is with a deep sense of responsibility that the National Strategy to Address Tech-Facilitated Gender-Based Violence 2026–2030 is presented. Pakistan’s rapid digital transformation has expanded access to information, services, and economic opportunities, particularly for women and girls. At the same time, the misuse of digital technologies has created new and complex forms of violence that threaten constitutional guarantees of dignity, equality, and personal security.

The Government of Pakistan recognizes that technology-facilitated gender-based violence is not merely a technological concern. It is rooted in structural inequalities and discriminatory social norms that are replicated and amplified in digital spaces. Such violence undermines women’s participation in public, economic, and political life and often extends beyond online harm into physical, psychological, and socio-economic consequences.

This National Strategy reflects the Government’s firm commitment to safeguarding human rights in the digital sphere. Developed through extensive consultations with federal and provincial institutions, civil society, development partners, and survivors, the Strategy sets out a coordinated and comprehensive framework to strengthen prevention, protection, accountability, and response mechanisms. Particular emphasis has been placed on addressing legal and institutional gaps, enhancing platform accountability, and ensuring timely protection for survivors.

The Strategy aims to ensure that the fundamental rights enshrined in the Constitution of Pakistan apply fully and effectively within digital environments. Its successful implementation will require sustained collaboration among line ministries, regulatory authorities, law enforcement agencies, provincial governments, civil society, and international partners. Collective action is essential to ensure that digital technologies serve as instruments of empowerment, inclusion, and development rather than tools of harm and exclusion.

**Senator Azam Nazeer Tarar**

Federal Minister for Human rights

## MESSAGE BY THE SECRETARY



The National Strategy to Address Tech-Facilitated Gender-Based Violence 2026–2030 represents a significant step forward in Pakistan’s institutional response to the growing challenge of digital violence. The Ministry of Human Rights has led the development of this Strategy in fulfilment of its mandate to protect and promote fundamental human rights, with particular attention to women, children, and other vulnerable groups.

The Strategy is the outcome of a structured and consultative process involving federal and provincial authorities, statutory commissions, civil society organizations, subject-matter experts, and survivors of technology-facilitated abuse. This inclusive approach has ensured that the Strategy is grounded in evidence, responsive to lived realities, and aligned with national priorities and international human rights obligations.

To address the gap between digital participation and personal safety, the Strategy adopts a coordinated Prevention, Protection, Prosecution, and Response framework. It emphasizes institutional strengthening, improved inter-agency coordination, and survivor-centred service delivery. Key measures include the establishment of a National TFGBV Coordination Cell within the Ministry of Human Rights, enhancement of investigative and prosecutorial capacity, and the promotion of gender-responsive and trauma-informed practices across the justice system.

The Strategy also highlights the importance of regulatory and platform accountability, legislative reform, data-driven decision-making, and sustained public awareness. Through its implementation, the Ministry seeks to contribute to a justice system that is accessible, effective, and responsive to the evolving nature of technology-facilitated harms, ensuring meaningful protection of rights in the digital age.

**Mr. Abdul Khaliq Shaikh**

Secretary, Ministry of Human Rights

## MESSAGE BY THE UNDP RESIDENT REPRESENTATIVE



Pakistan's digital transformation is now an integral part of the country's development trajectory. It is reshaping how people access services, exercise rights, build livelihoods, and participate in public space. Digital transformation is no longer optional; it is a lived reality and a critical enabler of good governance. For this transformation to be truly inclusive, safety and dignity must be treated as core conditions of digital participation, not optional add-ons.

Technology-facilitated gender-based violence (TFGBV) risks undermining this inclusive digital transformation. When women and girls face harassment, abuse, or intimidation online, their ability to access services, pursue education and livelihoods, and engage in civic life is constrained. Digital progress cannot be considered inclusive or sustainable if half the population is silent or withdraws altogether. Addressing TFGBV is therefore central to Pakistan's digital agenda, ensuring that transformation delivers its development promise.

The National Strategy to Address Technology-Facilitated Gender-Based Violence (2026-30) recognizes both the opportunities and risks of a rapidly expanding digital landscape. In 2024, with eight million new female users added online, tangible progress in digital inclusion appears incrementally within reach. Yet the protection gap remains stark: the same year saw 135,000 cybercrime complaints, with only 826 cases proceeding to prosecution. Expanding digital access must be matched by credible, survivor-centred systems and institutions equipped to respond consistently and effectively.

UNDP Pakistan is honored to support the Ministry of Human Rights in formulating this Strategy and commends its leadership in stewarding this important national effort. Developed through a consultative process, including the Technical Working Group on TFGBV, the Strategy reflects contributions from stakeholders across justice, law enforcement, regulatory, education, and human rights institutions, alongside civil society, survivor-support actors, UN partners, and digital rights organizations. It establishes a comprehensive framework to address TFGBV as part of a broader effort to combat gender-based violence (GBV), and to guide a coordinated response grounded in rights, dignity, and equality.

Any strategy's success is ultimately defined by its implementation. Advancing this agenda will require committed leadership, adequate resourcing, effective coordination and accountability, alongside the agility to respond to evolving technologies and patterns of harm.

UNDP is committed to working with the Government of Pakistan and partners to translate this strategy into measurable progress, ensuring that women and girls can participate online and offline without fear, and that Pakistan's digital future is inclusive and equitable.

**Dr. Samuel Rizk**  
Resident Representative  
UNDP Pakistan

## **VISION**

To foster a safe, inclusive, and rights-based digital environment in Pakistan where women, girls, and marginalized communities are able to participate fully and confidently in digital life without fear of violence, harassment, or exploitation, and where constitutional guarantees of dignity, equality, and security are upheld across all digital spaces.

## **MISSION STATEMENT**

To prevent and eliminate tech-facilitated gender-based violence through a coordinated and survivor-centred national framework that strengthens legislative and regulatory protections, enhances institutional and justice-sector capacity, ensures accountability of digital platforms, and promotes social and behavioural change, thereby safeguarding the human rights of women and vulnerable groups in Pakistan's digital ecosystem.

## EXECUTIVE SUMMARY

The National Strategy for Addressing Technology-Facilitated Gender-Based Violence (TFGBV) 2026-2030 represents Pakistan's first comprehensive framework to address the growing crisis of digital violence against women, girls and marginalised communities in the country. As Pakistan's digital landscape rapidly expands, with 8 million women coming online in 2024 alone, the urgency of protecting women's digital rights has never been more critical. This strategy responds to the alarming reality of technology-facilitated violence which has become a tool of gender-based oppression, forcing women and marginalised to choose between digital participation and personal safety.

The strategy acknowledges that TFGBV is not merely a technological challenge but a manifestation of deep-rooted patriarchal structures that have found new expression through digital platforms; TFGBV creates a continuum of violence that extends from digital spaces into physical harm, socio-economic exclusion, and silencing of women's voices in political spheres.

Built on extensive stakeholder consultations, survivor testimonies, and institutional analysis, this strategy establishes a multi-sectoral response framework that addresses the complete ecosystem enabling TFGBV, from legal and enforcement gaps to platform accountability and underlying patriarchal norms. It creates specialised institutional mechanisms including a National TFGBV Coordination Cell, female officers led dedicated investigation units within National Cyber Crimes Investigation Agency (NCCIA), and support services that prioritise survivor dignity and safety. The strategy further mandates platform accountability through regulatory frameworks while addressing root causes through nationwide awareness campaigns targeting toxic masculinity and promoting inclusive digital citizenship.

The five-year roadmap commits Pakistan to transforming its justice system's response to TFGBV, ensuring that women, and marginalised communities' constitutional rights to dignity, equality, and participation extend fully into digital spaces, ultimately enabling their equal participation in Pakistan's digital future.

# KEY OBJECTIVES

## 1. Strengthen Legislative Frameworks

- Enact TFGBV-specific legislation that clearly defines and criminalises all forms of technology-facilitated gender based violence
- Establish specialised regulatory mechanisms through SMPRA with 24-hour content removal mandates and platform accountability measures
- Develop investigation, prosecution guidelines and judicial protocols for processing TFGBV cases

## 2. Whole of Government Approach

- Establish female officers led specialised TFGBV units in all districts within NCCIA police stations
- Create integrated support services including 24/7 emergency reporting helpline, digital reporting and verification mechanisms within NCCIA
- Develop digital evidence handling SOPs to protect survivor dignity and prevent re-victimization during investigations

## 3. Ensure Platform Accountability and International Cooperation

- Mandate emergency data-sharing protocols for social media platforms for high-risk TFGBV cases
- Establish formal regulation mechanisms of social media platforms through SMPRA
- Advocate for Global South perspectives in international platform governance forums

## 4. Transform Social Norms and Prevent Violence

- Implement nationwide awareness campaigns addressing toxic masculinity and promoting respectful, inclusive digital citizenship
- Integrate TFGBV prevention in educational curricula and community-based programs
- Engage religious and community leaders in promoting women's digital rights

### **5. Establish Coordination and Implementation Mechanisms**

- Create National TFGBV Coordination Cell for inter-agency collaboration
- Develop digital data collection systems with gender-disaggregated statistics within NCCIA and SMPRA
- Implement feedback integrated monitoring and evaluation frameworks

# 1 EXPECTED OUTCOMES

## 1. Strengthen Legislative Frameworks

*Objective 1.1: Enact TFGBV-specific legislation that clearly defines and criminalises all forms of technology-facilitated gender-based violence*

### Expected Outcomes:

- Dedicated TFGBV legislation enacted providing legal definition for TFGBV, criminalising, doxing, online blackmail, image-based abuse, misogynistic hate speech, impersonation and other forms of digital violence
- Legislation criminalises harms associated with AI-generated content including deepfakes audios, videos
- Enhanced penalties for repeated offenders of TFGBV

*Objective 1.2: Establish specialised regulatory mechanisms through SMPRA with 24-hour content removal mandates and platform accountability measures*

### Expected Outcomes:

- 24-hour content removal mandated for emergency TFGBV cases involving intimate image abuse and viral harassment
- Dedicated TFGBV reporting channels within the Council staffed by trained female personnel
- Platform compliance framework implemented, standardising response across all platforms

*Objective 1.3: Develop investigation, prosecution guidelines and judicial protocols for handling TFGBV cases*

**Expected Outcomes:**

- Standardised investigation protocols for TFGBV cases, with digital evidence collection SOPs implemented across NCCIA police stations
- Specialised prosecution guidelines developed for digital evidence presentation, technical aspects of TFGBV cases
- Trauma-informed court procedures established including video link testimony options, expedited hearing timelines, and sentencing guidelines reflecting psychological harms associated with TFGBV

**2. Whole of Government Approach**

*Objective 2.1: Establish specialised female officers led TFGBV units within NCCIA Police Stations in all districts*

**Expected Outcomes:**

- NCCIA personnel strength increased from current 200 to 2500+ officers with 30:70 gender ratio target, ensuring adequate female officers' representation for TFGBV investigations
- Female officers led TFGBV investigation units operational in all districts nationwide
- Specialised survivor centered training programs implemented for all TFGBV investigators covering digital evidence collection, platform-specific technical aspects, and understanding of honour-based violence escalation patterns
- SDPO-level cybercrime units established with staff trained specifically in handling cybercrimes and sensitive digital evidence collection, ensuring first-point police contact effectively responds to TFGBV reports
- Digital Case Transfer Management System created to ensure streamlined TFGBV complaint transfer from local police to NCCIA

*Objective 2.2: Create integrated support services including 24/7 emergency reporting helpline, digital reporting and verification mechanisms, and trauma-informed response protocols*

**Expected Outcomes:**

- Nationwide multilingual NCCIA 24/7 reporting helpline functional, linking 1099 (MoHR), 15 (Police), and NCSW helpline to the national cybercrime helpline
- NCCIA online reporting portal and mobile app deployed with digital complaint verification mechanism
- Psychosocial support services established with female staff across all service points within NCCIA police stations, addressing intersectional vulnerabilities including disability, transgender identity, and language barriers

*Objective 2.3: Develop evidence handling SOPs protecting survivor dignity and preventing re-victimization*

**Expected Outcomes:**

- Digital Evidence handling Standard Operating Procedures implemented specifically addressing sensitivities associated with TFGBV cases
- Digital case management system operational with human supervised AI-assisted case classification prioritising intervention based on severity and urgency indicators
- Trauma-informed protocols implemented during investigation proceedings, with dedicated private interview spaces, and confidentiality safeguards

**3. Ensure Platform Accountability and International Cooperation**

*Objective 3.1: Mandate emergency data-sharing protocols with social media platforms for high-risk TFGBV cases*

**Expected Outcomes:**

- Emergency 24-hour Basic Subscriber Information (BSI) sharing protocols implemented for high-risk TFGBV cases involving intimate image abuse, deepfakes, or credible threats of offline violence
- Standardised data-sharing protocols established with verified government requests, clear timelines, and requirements

- Platform emergency coordination mechanisms operational with focal points for high-risk cases requiring immediate intervention
- Real-time tracking systems deployed with unique reference numbers, status updates, and estimated review timelines for all TFGBV cases

*Objective 3.2: Establish formal regulation mechanisms of social media platforms through Social Media Protection and Regulatory Authority*

**Expected Outcomes:**

- Graduated platform accountability system operational with performance-based compliance scoring, warnings, fines for repeated non-compliance
- Annual compliance reports mandated for platforms operating in Pakistan, with regular audits on response and cooperation
- Safety by Design requirements mandated including automated detection systems for non-consensual intimate image abuse, deepfake detection, and tools for countering misinformation that perpetuates TFGBV

*Objective 3.3: Advocate for Global South perspectives in international platform governance forums*

**Expected Outcomes:**

- Bilateral cooperation established with platform headquarters countries addressing transnational challenges
- Regional coalition built with South Asian and MENA countries for collective platform accountability, leveraging shared cultural contexts and legal frameworks to strengthen negotiating position
- International advocacy initiatives launched ensuring Global South perspectives are integrated into platform governance frameworks and community guidelines

#### 4. Transform Social Norms and Prevent Violence

*Objective 4.1: Implement nationwide awareness campaigns addressing toxic masculinity and promoting respectful, inclusive digital citizenship*

##### **Expected Outcomes:**

- Behaviour Change Communication (BCC) campaigns addressing toxic masculinity launched across urban and rural areas
- Influencer and celebrity partnerships established through social media campaigns challenging misogynistic hostility and promoting inclusive digital citizenship
- Nationwide awareness campaigns on digital safety for women and marginalised communities initiated

*Objective 4.2: Integrate TFGBV prevention in educational curricula and community-based programs*

##### **Expected Outcomes:**

- Mandatory 3 credit-hour TFGBV awareness module integrated across all HEC academic disciplines with contextualised digital safety education
- Updated mass communication curricula implemented at BS and postgraduate levels covering device ownership, privacy settings, recognising harassment, and reporting digital abuse to relevant departments
- Digital safety resource centres operational in major universities, colleges, high schools and community centres providing training, support, response resources, and expert guidance for navigating digital spaces safely

*Objective 4.3: Engage religious and community leaders in promoting women's digital rights*

##### **Expected Outcomes:**

- Religious and traditional leaders across all provinces engaged to **advance** women's digital rights **through community-aligned approaches**

- Community-based interventions, leveraging polio and lady health worker networks, implemented to address harmful gender stereotypes, including those around trans-persons, to create digital rights and safety awareness

## 5. Establish Coordination and Monitoring Mechanisms

*Objective 5.1: Create National TFGBV Coordination Cell for inter-agency collaboration*

### Expected Outcomes:

- National TFGBV Coordination Cell operational within Ministry of Human Rights with dedicated staffing, providing centralised coordination between federal and provincial authorities for consistent TFGBV response across Pakistan
- Permanent inter-ministerial working groups established linking Ministry of Human Rights, IT & Telecom, Law & Justice, Interior, Commerce, Education and relevant Commissions (national and provincial - NCHR, NCSW, NCRC) ensuring policy alignment and resource coordination
- Dedicated civil society, including disabled persons, advisory positions created, enabling community perspectives to inform policy development and implementation adjustments

*Objective 5.2: Develop digital data collection systems for technology facilitated crimes with gender-disaggregated statistics*

### Expected Outcomes:

- Gender-disaggregated digital data collection systems for technology facilitated crimes implemented across NCCIA, PTA/SMPRA and prosecution authorities
- Performance indicator tracking system made operational, monitoring the conversion of TFGBV complaints into FIRs and convictions
- Regular trend analysis conducted enabling evidence-based policy adjustments and targeted interventions

*Objective 5.3: Implement survivor feedback integrated monitoring and evaluation frameworks*

**Expected Outcomes:**

- Monitoring framework operational, tracking progress against baseline statistics including prosecution success rates, response times and platform compliance
- Survivor feedback mechanisms institutionalised through regular consultation processes with survivors of TFGBV and civil society organisations
- Federal-provincial coordination mechanisms operational across all provinces for consistent TFGBV response standards, resource allocation, and performance monitoring

This strategy represents Pakistan's commitment to ensuring that digital transformation promotes women's and Marginalised communities' rights, creating an inclusive digital ecosystem where all citizens participate equally, safely, and with dignity in the nation's digital future

## **1. BACKGROUND AND CONTEXT**

### **1.1. Spectrum of the Issue**

Pakistan's digital landscape has undergone rapid transformation, with the country of 240 million witnessing an unprecedented increase in women's digital participation; 8 million new female users came online in 2024 alone. Yet this historic progress is shadowed by a growing crisis: tech-facilitated gender-based violence that threatens to transform digital opportunity into digital harm for millions of women.

Technology-Facilitated Gender-Based Violence (TFGBV), as defined by the UN Special Rapporteur, encompasses any act of gender-based violence against women that is committed, assisted, or aggravated by the use of Information and Communication Technology. In Pakistan, such violence manifests through multiple forms including doxxing, cyber harassment, image-based abuse,

blackmail, and AI-generated deepfakes, frequently escalating into serious offline consequences.

Understanding these specific manifestations is critical to developing effective responses. TFGBV operates through multiple, often intersecting forms of abuse. **Doxxing** involves the malicious publication of private information including addresses, phone numbers, or workplace details to facilitate offline harassment or threats. **Cyber harassment** encompasses repeated unwanted contact, threatening messages, and coordinated abuse campaigns that create hostile digital environments, forcing women to self-censor or withdraw from online spaces. **Misogynistic hate speech** targets women with gendered slurs, rape threats, and violent imagery designed to silence women's voices in public discourse, particularly affecting women in visible positions including activists, journalists, and public figures.

Beyond harassment, TFGBV escalates into coercive and exploitative forms that directly threaten women's safety and autonomy. **Online blackmail and threats** leverage intimate images, private conversations, or fabricated content to coerce survivors into silence, compliance, or extortion, resulting in severe psychological and at times, physical harm. **Image-based abuse** includes the non-consensual creation, distribution, or threatened distribution of intimate or sexual images, increasingly facilitated by AI-generated deep fakes that superimpose victims' faces onto explicit content without their knowledge or consent. **Impersonation** creates fake profiles or accounts using victims' identities to damage reputations, share false information, or facilitate further abuse.

In Pakistan's patriarchal context, these forms of TFGBV rarely exist in isolation. They often intersect and escalate in dangerous patterns, with digital abuse serving as a precursor to honour-based violence, forced marriage, or femicide. This escalation transforms TFGBV from a technological challenge into a threat to women's physical safety, socio-economic participation, and fundamental rights. The continuum of violence from online harassment to offline harm demands a systems-wide response: one that spans platform regulation, legal frameworks, institutional capacity, and societal transformation in how Pakistan understands and addresses gender-based violence in the digital age.

The scale of the issue in Pakistan becomes evident when examining the country's institutional response to technology-facilitated gender-based violence. In 2024, the National Cyber Crime Investigation Agency (NCCIA) received 135,000 cybercrime complaints, yet only 826 cases proceeded to prosecution, representing a mere 0.6% success rate. This alarming statistic underscores the deficiencies in Pakistan's current response mechanisms, where the vast majority of victims receive no meaningful legal recourse once they approach the criminal justice system.

The access to justice limitations are equally concerning. Pakistan's entire population of 240 million is served by only 15 cybercrime police stations across the country, each requiring mandatory in-person verification for complaint registration. This geographic centralisation creates insurmountable barriers for women and vulnerable communities, particularly those residing in rural areas. Beyond geographic barriers, human resource constraints make effective response unattainable, with approximately 200 NCCIA officers handling on average over 135,000 complaints annually, resulting in a caseload of more than 900 complaints per officer each year.

The digital dependency patterns among Pakistani women creates additional vulnerabilities. Approximately 35% of women depend on borrowed mobile devices, primarily from male family members, severely limiting their ability to safely report abuse or seek help without risking further violence or family conflict. This device dependency intersects with cultural factors to create a form of vulnerability where women cannot maintain the privacy necessary to document abuse or communicate with support services.

The Regulatory mechanisms face parallel challenges. The Pakistan Telecommunication Authority (PTA) received 1.5 million complaints in 2024 but were able to address only 100,000. Additionally, the authority does not maintain gender-disaggregated data, making it difficult to track TFGBV-specific trends or develop targeted interventions.

The convergence of limited access to justice, resource constraints, and cultural

barriers creates an environment where perpetrators operate with near-complete impunity while survivors are left without legal recourse. This reality demands immediate reform through a national strategy that addresses the direct and the structural causes of technology-facilitated gender-based violence in Pakistan.

## **1.2. Constitutional Framework**

Pakistan's Constitution provides the basis and guarantees that directly support the right to digital safety and protection from tech-facilitated gender-based violence. Article 9 ensures that no person shall be deprived of life or liberty except in accordance with law, establishing the foundational right to security that extends to digital spaces where online threats often escalate to offline violence. Article 14 guarantees the inviolability of human dignity and privacy of the home, protections that must evolve to encompass digital dignity and online privacy in an increasingly connected world. Article 25 mandates equality before law and equal protection for all citizens, explicitly prohibiting discrimination on the basis of gender while permitting special provisions for the protection of women and children. These constitutional provisions, read together with Article 4's guarantee of the right to be dealt with in accordance with law, create a strong legal basis to address TFGBV through legislative, institutional, and enforcement mechanisms that would ensure women's and vulnerable communities' full and equal participation in Pakistan's digital future.

## 2

## INTERNATIONAL OBLIGATIONS AND COOPERATION

Given that technology-facilitated violence often transcends national boundaries, the strategy addresses both the Convention on the Elimination of All Forms of Discrimination against Women commitments and the urgent need for collaborative frameworks with other nations. The measures outlined below will strengthen Pakistan's domestic response while contributing meaningfully to regional and global efforts to combat technology-facilitated gender-based violence.

### 2.1. CEDAW Alignment

This strategy directly supports Pakistan's obligations under the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), particularly General Recommendation 35 on gender-based violence, which recognizes technology-facilitated violence as a contemporary form of discrimination requiring state action. The CEDAW Committee has consistently emphasized that state parties must address online and ICT-based violence through legislative reform, institutional mechanisms, and access to justice frameworks. By establishing comprehensive prevention, protection, and accountability measures for TFGBV, Pakistan fulfils its commitment to eliminate all forms of gender-based violence. The strategy further integrates Pakistan's CRPD commitments, ensuring accessible justice pathways and barrier-free digital participation for women and girls with disabilities.

### 2.2. Transnational Linkages

Technology-facilitated gender-based violence increasingly operates across borders, requiring coordinated international response mechanisms. TFGBV intersects with transnational threats including human trafficking networks, with digital platforms frequently misused for exploitation, grooming, and extortion particularly targeting vulnerable populations and gender minorities. Addressing these cross-border challenges requires strengthened international cooperation, including bilateral agreements with jurisdictions hosting major platforms to facilitate evidence sharing, coordinate TFGBV investigations, and enable content removal.

## 3 LEGISLATIVE FRAMEWORK

Pakistan's approach to digital governance began with the Telegraph Act, 1883, which established government authority over telecommunications infrastructure, from telegraphy to radio communications. While this Act provided control over traditional communications technology, it could not anticipate or address the complexities of 21st-century digital crime. This legislative inadequacy led to the Prevention of Electronic Crimes Act 2016 (PECA), purpose-built legislation for combating contemporary cyber offenses.

### 3.1. PECA 2016-2025

The Prevention of Electronic Crimes Act 2016 was designed to address cyber harassment, including violence against women, and has undergone two amendments since its enactment. However, implementation challenges and certain structural limitations in key sections continue to constrain **effective** prosecution of TFGBV cases. Section 20, which criminalizes offences against dignity is undermined by what practitioners term the *blackmail loophole*; the law requires content to be "exhibited," "displayed publicly," or "transmitted" to constitute an offense, meaning perpetrators who threaten to share intimate content without publishing it face no criminal sanctions. This narrow focus does not recognise that the threat itself causes serious psychological harm and coercion, a common tactic in technology-facilitated blackmail. The section's effectiveness is further undermined by social media platforms' refusal to share data with investigation agencies, particularly in cases involving anonymous perpetrators, bringing investigations to a standstill regardless of the severity of harm. Section 16, addressing identity theft through impersonation and doxxing, faces dual barriers: its non-cognizable status requires court orders for investigation, while platforms frequently decline requests for crucial identification data, leaving complaints trapped in procedural delays. Section 21, which deals with offenses against modesty including intimate image abuse and the emerging threat of deepfakes, shows greater clarity in defining offense parameters but remains hampered in its effectiveness by the same blackmail loophole and platform non-cooperation. Despite being non-compoundable, meaning victims cannot settle with accused parties, the lengthy legal

procedures often result in informal compromises outside the court system, while limited data sharing by platforms continues to obstruct case registration against anonymous perpetrators.

While PECA 2016 and its subsequent amendments represent Pakistan's efforts to address technology-facilitated crimes, the deficiencies outlined above underscore the urgent need for dedicated TFGBV-specific legislation. Piecemeal amendments cannot adequately address the evolving nature and severity of technology-facilitated gender-based violence. Such legislation must clearly define TFGBV in all its manifestations, explicitly criminalise threats of publication alongside possession and distribution of such content, and address AI-generated content including deepfakes.

### **3.2 . PECA Amendment 2025 - New Regulatory Framework:**

The PECA Amendment 2025 introduces a three-tier regulatory structure that offers potential improvements for TFGBV response. The Social Media Protection and Regulatory Authority (SMPRA) serves as the primary regulatory body with powers to issue content removal orders within 24 hours; a substantive capability for preventing viral distribution of intimate images or harassment content. The Social Media Complaint Council functions as a complaints processing body that could potentially establish specialized TFGBV reporting channels with trained female personnel who understand the contextual realities. However, the Act does not clarify which complaints fall under the Authority versus the Council's jurisdiction, despite both being mandated with complaint-handling responsibilities. The third tier, Social Media Protection Tribunals, hear appeals against Authority decisions, but appeals from Tribunals go directly to the Supreme Court, bypassing High Courts entirely. This would create significant access barriers for ordinary litigants, particularly TFGBV survivors who may find Supreme Court proceedings expensive and complex. While the framework's 24-hour content removal mandate and potential for specialised complaint mechanisms represent improvements over the current systems, its ultimate effectiveness will depend on the prioritisation of victim protection, especially women and vulnerable communities.

The identified jurisdictional ambiguities and appeals procedures may be addressed through the implementing rules and regulations yet to be formulated for the Authority, Council, and Tribunals. This provides an opportunity to embed survivor-centered mechanisms from inception, including clear delineation of complaint-handling jurisdictions between the Authority and Council, and accessible appeals pathways that do not necessitate direct Supreme Court proceedings for TFGBV survivors.

## 4 INSTITUTIONAL FRAMEWORK

### 4.1. National Cyber Crime Investigation Agency (NCCIA)

Pakistan's institutional response to technology-facilitated gender-based violence reveals a system overwhelmed by scale, undermined by resource constraints, and dependent on the voluntary cooperation of platforms that operate beyond domestic jurisdiction. The transformation of the Federal Investigation Agency's Cyber Crime Wing into the National Cyber Crime Investigation Agency (NCCIA) in 2025 acknowledged the need for specialised capacity, yet this institutional restructuring has done little to address the fundamental barriers that limit the access to justice.

The geographic centralization of cybercrime police stations, resource challenges, and platform non-cooperation collectively create an environment where 65% of reported cybercrime complaints achieve no meaningful legal outcome, **resulting** in near-complete impunity for offenders in many cases.

#### Challenges:

- Geographic centralization with 15 cybercrime police stations serving 240 million people
- Mandatory in-person verification creates barrier to access justice
- Human and financial resource constraints with 200 officers handling on average 135,000 complaints annually

### 4.2. Platform Accountability Crisis

The investigation and prosecution of TFGBV cases in Pakistan **encounter** a structural barrier: social media platforms operate beyond the reach of domestic law enforcement, controlling access to evidence essential for criminal proceedings. While Pakistani authorities can investigate and prosecute technology-facilitated crimes, their effectiveness depends entirely on platforms' voluntary cooperation, a dependency that has created arbitrary enforcement where justice becomes a matter of corporate policy rather than legal merit. The disparities are stark: perpetrators using X (formerly Twitter) enjoy complete immunity due to the platform's zero compliance with Pakistani LEA's data requests since 2021, while those on Meta platforms face a 75% chance of

identification. This creates a *platform lottery system* where dispensation of justice depends on which platform perpetrators choose rather than legal merits of the case.

The enforcement lottery reflects a deeper structural conflict between global platform policies shaped by Global North regulatory norms and Pakistan's domestic criminal justice requirements. The absence of Mutual Legal Assistance Treaties with countries hosting major platforms compounds the issue, as companies cite this lacuna when declining data requests even in cases involving serious crimes such as intimate image abuse or credible threats of offline violence emanating from online engagements. Beyond individual data-sharing refusals, platforms' engagement-driven algorithms actively amplify gender-based attacks; research shows women face twenty-seven times more online abuse than men, reflecting design features that prioritise controversy over safety. Through both non-cooperation in investigations and algorithm-driven amplification of abuse, platforms create a system where TFGBV persists with impunity, leaving survivors without effective legal recourse.

#### **Platform Compliance Rates:**

- **Meta:** 75% compliance with data requests from Pakistani LEAs
- **X (Twitter):** 0% compliance since 2021 (17 requests, zero responses)
- **TikTok:** 16.3% compliance for legal requests from LEAs

### **4.3. Regulatory Framework: Pakistan Telecommunication Authority, Social Media Regulatory Authority, Council and Tribunal**

The PECA Amendment 2025 introduces a new regulatory framework that will replace PTA upon establishment offering potentially improved pathways for addressing TFGBV. The amendments establish a three-tier complaint review system for cyber issues: the Social Media Protection and Regulatory Authority (SMPRA), the Social Media Complaint Council, and Social Media Protection Tribunals. Although these bodies have been officially notified, they are yet to be established and operationalised.

**Strategic Opportunities:** The regulatory framework addresses critical timing dimensions of TFGBV harm through:

- SMPRA's 24-hour content removal mandate under Section 2C providing immediate relief to TFGBV survivors
- Potential for specialised TFGBV reporting channels through the Council
- Platform accountability mechanisms through compliance requirements

#### 4.4. Prosecution

The prosecution of cybercrimes is undermined by capacity and resource constraints. With only seven prosecutors nationwide at NCCIA handling cybercrime cases, prosecutors are confronted with overwhelming caseloads that result in significant delays even after investigations conclude. Prosecutors lack specialised training in digital evidence presentation, understanding of platform-specific technical aspects, and the nuanced nature of TFGBV crimes that often involve complex technological manipulation and anonymous perpetrators.

The absence of dedicated TFGBV prosecution units means these cases compete for attention with other cybercrimes, often receiving lower priority despite their severity. Furthermore, prosecutors struggle with presenting digital evidence effectively in court, particularly when dealing with AI-generated content, deepfakes, or cases involving multiple platforms and jurisdictions. The current prosecution framework requires fundamental reform including specialised TFGBV prosecution units, training on digital evidence and trauma-informed approaches, digital forensics, and clear prosecution guidelines that recognise the unique characteristics and severity of technology-facilitated gender-based violence.

#### 4.5. Judiciary

The judicial response to TFGBV reflects the same challenges identified above. Courts often struggle to comprehend the lasting psychological and social harm caused by digital abuse, particularly in Pakistan's context where online harassment frequently escalates to offline violence, social ostracization, and in extreme cases, honour killings. The absence of specialised courts for TFGBV cases means these matters are heard alongside general cybercrime cases, without recognition of their gender-based dimensions or the specific vulnerabilities of women survivors. The lengthy judicial procedures, combined

with the requirement for survivors to repeatedly recount traumatic experiences in open court without video link options, more than often leads to informal compromises outside the court system. The strategy requires establishing specialised TFGBV courts, trainings, implementation of trauma-informed court procedures including video link testimony options, expedited hearing timelines, development of sentencing guidelines that reflect the severe harm caused by TFGBV.

#### 4.6. Commissions

The three statutory commissions under the Ministry of Human Rights, the National Commission for Human Rights (NCHR), National Commission on the Status of Women (NCSW), and National Commission on the Rights of Child (NCRC) and their provincial counterparts, play crucial oversight and advocacy roles in addressing TFGBV within Pakistan's human rights framework. The NCHR, established through the National Commission for Human Rights Act 2012, possesses judicial and investigative powers to conduct suo-moto inquiries, review existing legislation against human rights principles, and serve as a watchdog for constitutional safeguards in digital spaces. The NCSW, established in 2000 following Pakistan's Beijing Declaration commitments, specifically examines policies and programs affecting women's digital safety, monitors mechanisms for redressing violations of women's rights online, and sponsors research on technology-facilitated violence as an emerging gender issue requiring urgent policy attention. The NCRC, created under the National Commission on the Rights of Child Act 2017, addresses the particularly vulnerable population of children and adolescents who face digital violence, including cyberbullying, online grooming, and exploitation through digital platforms.

These commissions collectively provide essential functions including receiving and investigating TFGBV complaints through their regional offices, conducting research and maintaining gender-disaggregated data on digital violence, advising government on legislative reforms needed to address emerging forms of TFGBV, raising awareness about digital rights and safety, building capacity of stakeholders on trauma-informed responses, and ensuring Pakistan's

compliance with international human rights obligations including CEDAW's requirements on addressing technology-facilitated violence. Their integration into the TFGBV response framework through the proposed National TFGBV Coordination Cell in this strategy will ensure monitoring, evidence-based policy development, and coordinated advocacy for survivors' rights across federal and provincial levels.

## 5 POLICY ALIGNMENT AND INTEGRATION

The proposed National Strategy to address TFGBV aligns with and builds upon Pakistan's existing digital governance architecture, particularly the Digital Gender Inclusion Strategy developed by the Pakistan Telecommunication Authority (PTA). This strategy specifically complements the Digital Gender Inclusion Strategy's identified gaps in addressing digital violence.

Furthermore, the strategy aligns with the Digital Gender Inclusion Strategy's three-year action plan targets, particularly the mandate to achieve a 30% improvement in women's safety perception in digital spaces and establish mechanisms for regularly reviewing and updating policies to ensure gender-responsiveness. By building upon these existing commitments, the TFGBV strategy accelerates Pakistan's progress toward creating safer digital environments for women while maintaining institutional continuity and leveraging established multi-stakeholder partnerships.

Additionally, the National TFGBV Protection and Response Strategy builds upon, and advances Pakistan's broader gender equality commitments established through the National Gender Policy Framework 2025-2030. The Gender Policy Framework addresses barriers across six priority areas: governance, education, employment, political participation, health, and safety. The PPPR approach of this strategy directly supports the Gender Framework's Objective 6 on Safety and Security, which calls for ending gender-based violence and mainstreaming gender protection across systems.

### **Methodology**

The development of this strategy followed a consultative, participatory approach ensuring multi-stakeholder engagement and survivor-centred perspectives. The process commenced with a baseline assessment examining Pakistan's institutional response mechanisms, legal frameworks, and the scale of TFGBV across the country. This was followed by provincial and national consultations conducted across all four provinces, gathering insights from federal and provincial authorities, civil society organisations, and affected communities. A Technical Working Group was established at the Ministry of Human Rights,

comprising representatives from government institutions, civil society organisations, multilateral organisations, and survivors of TFGBV, ensuring diverse perspectives informed the strategy's development.

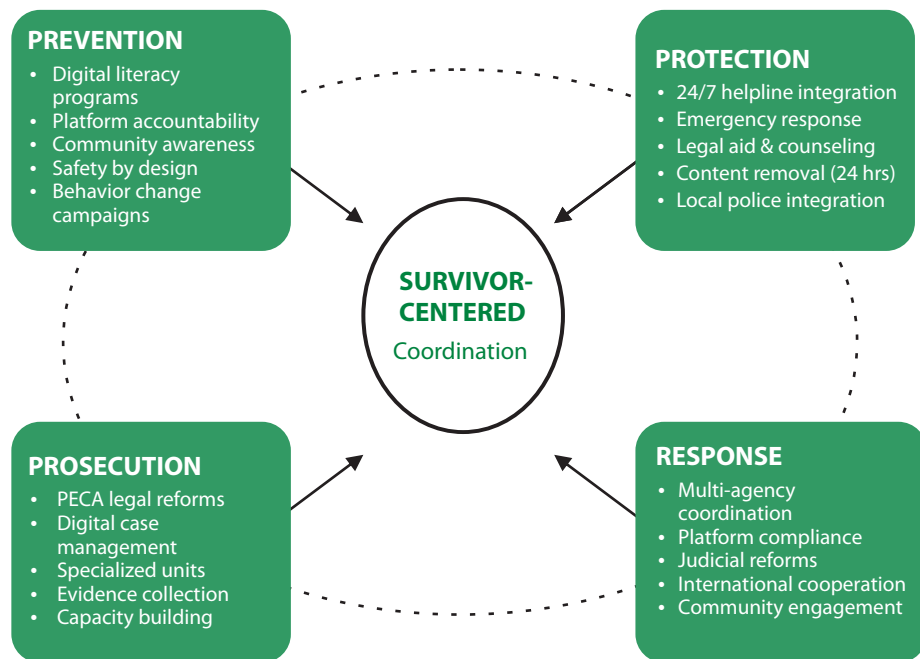
Through iterative consultations with the Technical Working Group, the strategy framework was developed, incorporating evidence-based interventions addressing Pakistan's specific institutional and cultural context. The draft strategy was subsequently circulated to all Technical Working Group stakeholders for detailed review, with feedback incorporated to strengthen the strategy's responsiveness to ground realities and ensure alignment with international best practices while maintaining contextual relevance for Pakistan's TFGBV response ecosystem.

# 6 STRATEGIC FRAMEWORK: THE PPPR APPROACH

Addressing TFGBV effectively requires moving beyond fragmented responses toward a coordinated, evidence-based system. The PPPR framework - Prevention, Protection, Prosecution, and Response - provides this methodology, built on international best practices while addressing Pakistan's specific institutional and cultural context. Each pillar is designed with multi-stakeholder integration and evidence-based interventions that address both immediate needs and institutional gaps. Given that Pakistan ranks 1.53 on a scale of 4-6 for women's access to justice, this participatory approach recognizes that effective TFGBV response requires contextualized survivor-informed interventions and civil society advocacy alongside government action.

## Pakistan's National TFGBV Strategy: PPPR Framework

A coordinated, Survivor-Centred Approach to Tech-Facilitated Gender-Based Violence



**Implementation Phases:**

- Phase-I: Legal reforms (0-6 months)
- Phase-II: Service Delivery (6-18 months)

**Current Crisis (2024 Baseline):**

- 0.6% prosecution success rate (826/135,000 complaints)
- 65% of complaints achieve no meaningful outcome

**Target Outcomes (2-year):**

- 15% prosecution success rate
- <20% cases with no meaningful outcome

## 6.1. PILLAR 1: PREVENTION

Effective prevention of TFGBV requires a three-pronged approach: building digital literacy and awareness, enforcing platform accountability, and implementing robust digital safety protocols. Prevention is as critical as response in addressing TFGBV, requiring proactive strategies that address not only Pakistan's digital gender divide but also create safer digital environments for inclusive digital participation.

### A) Digital Literacy and Awareness

#### Prevention Programs Addressing Digital Gender Divide:

Prevention strategies will address Pakistan's digital gender divide, where male social media usage stands at 78% while female usage remains at only 47%, creating digital environments where women face disproportionate risk of abuse. With 35% of women depending on borrowed mobile devices, digital literacy programs will prioritize device ownership, information on privacy settings, and recognizing early warning signs of online harassment.

Specific Interventions:

#### 1. Curriculum Integration:

- **Mandatory 3 credit-hour module** under General Education cluster across all academic disciplines
- **Digital Safety literacy** addressing TFGBV in Pakistan with local, contextualized content in Schools, Colleges and Universities
- **Updated mass communication curricula** (undergraduate and postgraduate levels)
  - Device ownership, privacy settings, and recognizing harassment
  - Reporting digital harassment/abuse to relevant departments

#### 2. Behaviour Change Communication (BCC):

- **Address generational gaps** in attitudes and behaviours through targeted family and peer group interventions with culturally sensitive approaches
- **Work with religious leaders, community elders and parents, local influencers, and traditional authority figures** to address harmful gender

stereotypes and promote women's digital rights within culturally sensitive frameworks that resonate with local communities

- **Revitalise school social work implementation** for early prevention
- **Introduce Teacher Training Programs** on digital safety, and online ethics
- **Early prevention and empowerment programs** targeting adolescent children, including male children

### 3. Public Awareness Campaigns:

- **Collaborate with PTA, HEC, and partners** using SMS, short videos, and community sessions
- **Engage influencers, celebrities, and sports personalities** for youth outreach
  - **Focus on men, specifically youth and vulnerable groups** to challenge misogynistic hostility/toxic masculinities
  - **Challenge Pakistan's victim-blaming culture** that characterises society's response to TFGBV

Beyond individual skills, multi-level prevention mechanisms will target communities and institutions through safety education programs addressing misogynistic hostility in digital environments. Prevention campaigns will recognize that TFGBV affects not only women and girls but also adolescent children, including male children who must be included in prevention initiatives.

### B) Platform Accountability and Industry Engagement

Given the enforcement crisis where platforms such as X maintain zero compliance with Pakistani data requests while Meta provides 75% compliance, prevention requires mandatory cooperation frameworks with social media platforms.

#### Mandatory Cooperation Frameworks:

- **Safety by Design** - Automated detection systems for non-consensual intimate image abuse, impersonation and circulation of other harmful TFGBV content

- **AI tools for myth-busting and fact-checking** to counter misinformation that perpetuates TFGBV
- **Simple, transparent, and trackable reporting mechanisms** for female users on platforms
- **Mandatory platform upgrades for deepfake detection** (addressing crisis where 95% of deepfake sexually explicit content is of women)
- **Standardized data-sharing protocols** with verified government requests specific to TFGBV
- **Performance-based compliance scoring** for platform accountability

### C) Digital Safety Protocols

#### Institutional Implementation:

- **Digital safety resource centres in universities, colleges, schools, community centres, and women's organizations** providing training, support, response resources, and expert guidance on navigating digital spaces safely
- **Inter-agency coordination mandates** to ensure timely interventions when required
- **Emergency response protocols** establishing coordination mechanisms with police, particularly cybercrime focal points within Virtual Women Police Stations or AIG Gender units in all provincial police departments

## 6.2. PILLAR 2: PROTECTION

Protection mechanisms address critical timing issues in current response systems that allow intimate images and harassment content to spread virally before intervention from relevant agencies. These protocols account for Pakistan's specific context, where online harassment often escalates to offline violence, requiring integrated safety planning around TFGBV cases.

## A) Immediate Response Mechanisms

### Leveraging PECA 2025 and Emergency Protocols:

- **Leverage SMPRA's 24-hour content removal mandate** under PECA 2025 for timely intervention
- **Emergency protocols addressing online-to-offline violence escalation** with coordination mechanisms
- **Coordination with existing institutional frameworks** including:
  - PSCA's emergency services networks – Virtual Women Police Station
  - PTA's regulatory mechanisms
  - MoHR's protection services and helpline
  - NSCW helpline
  - PM's Portal
- **Emergency response for high-risk situations** including suicide threats and imminent harm
- **Content removal and account suspension** in cases of criminal instances of TFGBV

### Regulatory Framework Integration:

- Clear division of responsibilities between SMPRA (platform regulation) and Council (complaint processing)
- Mandatory TFGBV expertise within Council structure
- Integration with NCCIA for criminal referrals when appropriate

## B) Survivor-Centric Support Services

Protection requires specialised services addressing the unique impacts of TFGBV in Pakistan's context, where survivors face family opposition, victim-blaming, and social stigma alongside digital abuse.

### Support Framework:

- **Legal aid, counselling, and rehabilitation services** addressing the unique impacts of TFGBV across diverse contextual realities in Pakistan's five provinces
- **Address intersectional vulnerabilities** particular to Pakistan, including:

- Linguistic minorities requiring multilingual support
- Women with disabilities needing accessible services
- Economically disadvantaged survivors who cannot afford travel costs to distant cybercrime stations
- Survivors facing family opposition and social stigma
- **Support for survivors facing family opposition, victim-blaming, and social stigma** alongside digital abuse
- **Psychosocial support and access to female staff** across all service points with the justice system
- **Coordinated local police response** for cases requiring immediate intervention beyond digital platforms

#### **SMPRA Integration for Rapid Response:**

- Leverage SMPRA's 24-hour content removal mandate for immediate protection
- Establish dedicated TFGBV reporting channels within the Council structure
- Develop specialised protocols for high-risk cases requiring emergency intervention
- Create fast-track procedures bypassing lengthy criminal justice processes for immediate relief

### **C) Legal Protection and Confidentiality Safeguards**

Protection frameworks address the legal gaps in the existing sections of the relevant law for TFGBV, and the procedural law, including but not limited to non-criminalisation of threats of publication, a common form of technology-facilitated blackmail where the threat itself causes serious psychological harm and coercion, and repeated online harassment.

#### **Legal Protection:**

- **Include a comprehensive definition of TFGBV in the law** - outlining the contours of the crime in clear terms and the types of offences, enhanced penalties for repeat offenders
- **Strengthen procedural law** to enable effective prosecution of TFGBV offences

- **Safe reporting mechanisms with privacy protection guarantees** to build trust and encourage reporting
- **Trauma-informed court procedures** minimising re-victimisation during lengthy legal proceedings by introducing video link options for survivors
- **Strengthen print and electronic media regulations** to prohibit the dissemination and publication of technology-facilitated gender-based violence content
- **Ensure evidence integrity** throughout investigation processes by introducing detailed standard operating procedures to handle sensitive digital evidence

#### **D) Local Police Integration - First Point of Contact**

Recognising that most citizens go to their local police first, especially in areas outside major cities, the strategy mandates mechanisms for case transfer between local police and NCCIA.

- **Establish cybercrime units at Sub-Divisional Police Officer level** with staff trained specifically in handling cybercrimes and sensitive digital evidence collection
- **Train local police staff with survivor-sensitive protocols** equipping them to respond and process TFGBV through relevant channels
- **Develop Digital Case Transfer Management System** to ensure streamlined transfer of complaints related to technology facilitated crimes from local police to NCCIA

#### **National Police Bureau Coordination Guidelines:**

Leveraging National Police Bureau's mandate for national-level police coordination and gender-responsive policing, the strategy recommends establishing a federal-provincial LEA coordination mechanism

- **Standardized case transfer guidelines** defining clear criteria for transfer from local police stations to NCCIA once a complaint is identified as technology-facilitated crime

**Accessible Reporting Mechanisms:**

- **Digital complaint-sharing mechanism with NCCIA, down to police station level** for improved accessibility
- **Public awareness on reporting options, including** platform reporting, NCCIA, local police, and regulatory frameworks, to inform survivors of available pathways to report
- **Gender-balanced recruitment (30:70 ratio target)** to address human resource capacity constraints - ensuring specialised TFGBV units have enough female officers across Pakistan
- **Protocols for digital evidence collection at local police level** - maintaining proper chain of custody

**6.3. PILLAR 3: PROSECUTION**

Prosecution efforts address the geographical limitations and human resource crisis where approximately 200 investigation officers handle 135,000 complaints annually, creating impossible caseloads of over 900 complaints per officer at the NCCIA.

**A) Investigation and Evidence Collection****Digital Case Management System:**

- **Tiered response system for priority-based case management** for effective resource allocation given current constraints where heinous cases of TFGBV involving threats to life, sharing of non-consensual intimate imagery, and cases with imminent risk of offline violence receive priority redressal and expedited investigation
  - **Critical Priority (0-24 hours):** Immediate threats to life, suicide ideation, non-consensual intimate imagery with viral potential, child sexual exploitation, credible physical violence threats
  - **High Priority (24-72 hours):** Sexual harassment with evidence, stalking patterns, doxxing with safety implications
  - **Medium Priority (3-7 days):** Identity theft, impersonation without immediate safety threats, harassment without explicit threats

- **Standard Priority (7-14 days):** Defamation, minor harassment, fake profiles without associated threats, general privacy violations
- **Human Supervised AI-assisted classification to prioritize cases based on severity, risk factors, and urgency indicators** - with human oversight, through designated posts to monitor the case influx 24/7 - ensuring high-risk cases involving threats of honour-based violence receive immediate attention within 2-4 hours
- **Standardized protocols for digital evidence collection and preservation** ensuring case integrity and survivor privacy.

## **B) Capacity Building and Resource Allocation**

### **Infrastructure and Human Resources:**

- **Increase NCCIA's Human Resource Capacity**, especially female investigation officers
- **Establish graduated budget allocation framework for TFGBV investigations** with differentiated funding slabs corresponding to case complexity
- **Technological infrastructure upgrades** including secure digital evidence storage systems, case management platforms, digital forensics laboratories
- **Trainings for prosecutors on presenting digital evidence** to improve conviction rates
- **Specialised training programs** for investigation of TFGBV cases, including trauma-informed survivor-centered protocols
- **Develop a centralised digital dashboard** to collect gender-disaggregated data on TFGBV reporting, investigation, and prosecution
- **Designated Police Station buildings** with adequate material resources for cybercrime police stations across Pakistan

## **C) Legal Framework and Procedural Reforms**

Current law requires content to be "exhibited," "displayed publicly," or "transmitted" to constitute offense, excluding common technology-facilitated blackmail scenarios where the threat itself causes psychological harm.

**Legislative Reforms:**

- **Explicit criminalisation of threats of publication** where the threat itself causes psychological harm
- **Dedicated TFGBV section within PECA** providing comprehensive legislative framework
- **Mandatory platform data-sharing provisions** ending the current "platform lottery" system
- **Streamlined reporting mechanisms** across different law enforcement agencies to reduce victim re-traumatization.

**D) Inter-Agency Data Sharing and Coordination**

The strategy addresses existing legal and regulatory challenges in data and information sharing between Federal Investigation Agency (FIA), National Cyber Crime Investigation Agency (NCCIA), and Provincial Police departments that currently impede effective case prosecution and victim protection.

**Coordination Mechanisms:**

- **Standardised protocols for coordination and information sharing** between local law enforcement, prosecutors, and federal authorities
- **Clear jurisdictional guidelines** for streamlined case management from initial reporting through final adjudication
- **Secure data transfer protocols** maintaining evidence integrity
- **Joint training programs** across all agencies involved in TFGBV response

**6.4. PILLAR 4: RESPONSE**

The response pillar establishes TFGBV sensitive frameworks addressing the current impunity crisis through coordinated action across judicial, institutional, platform, and social dimensions.

**A) Immediate Response****Survivor Centered Institutional Emergency Response:**

- **Emergency interventions for high-risk cases** with 24-hour response competency

- **24-hour platform response for offline threats** coordinating with social media platforms for heinous TFGBV cases
- **Emergency 24-hour BSI sharing protocols for TFGBV cases** mandating platforms to provide Basic Subscriber Information within 24 hours for high-risk TFGBV cases involving intimate image abuse, deepfakes, or credible threats of offline violence
- **Crisis intervention protocols for imminent harm** including suicide ideation and threats to life
- **Rapid content removal and account suspension** through SMPRA mandate for high-risk TFGBV cases
- **Platform emergency coordination through focal points and trusted partners** for high-risk situations requiring immediate intervention

#### **Trackable Platform Response:**

- **2-hour acknowledgment requirement** for all TFGBV reports submitted to platforms
- **24-hour initial decision by platforms** with human review for appeals and clear explanation of platform policies and legal standards
- **Real-time case tracking systems** with unique reference numbers, status updates, and estimated review timelines for all TFGBV reports

#### **B) Judicial Response**

##### **Judicial System Reforms:**

- **Sentencing guidelines** reflecting severe psychological and social harm in TFGBV cases
- **Specialized Prosecution Units to handle TFGBV cases** within NCCIA structure
- **Performance metrics for judicial authorities** handling TFGBV cases with mandatory case hearing deadlines
- **Clear timelines and milestones for legal proceedings** in TFGBV cases to address current delays
- **Trauma-informed court procedures** minimizing re-victimization during proceedings including video link options

### C) Institutional Response

#### Agency Coordination Framework:

- **Agency coordination through National TFGBV Coordination Cell** within Ministry of Human Rights
- **Inter-ministerial working groups for policy alignment** linking Ministry of IT, Law & Justice, Interior, and relevant Commissions
- **Standardized protocols across law enforcement agencies** ensuring consistent response
- **Corrective measures for inadequate institutional responses** that contribute to inconsistent case outcomes
- **Functional inquiry mechanisms through NCSW and PCSWs** for TFGBV complaints
- **Dedicated civil society advisory positions** ensuring survivor-centred approaches
- **Representation of Disabled Persons Organizations (DPOs)** in the Coordination Cell and all design, monitoring, and evaluation processes
- **International cooperation protocols** for cross-border (transnational) digital crimes

### D) Platform Response

#### Platform Accountability Through the New Regulatory Framework:

- **Mandatory compliance frameworks through SMPRA** with focus on inconsistent cooperation by platforms operating in Pakistan
- **Emergency 24-hour BSI sharing protocols for high-risk TFGBV cases** involving intimate image abuse, deepfakes, or credible threats of offline violence
- **Standardised data-sharing protocols** for verified cases with clear timelines and requirements
- **International cooperation for cross-border enforcement** addressing transnational jurisdictional challenges

#### SMPRA Platform Oversight Powers:

- **Regulatory requirements** mandating platform-specific TFGBV trackable reporting categories in local languages

- **Real-time case tracking systems** with unique reference numbers and status updates
- **Transparent appeals processes** with review for TFGBV cases
- **Safety by Design approach** - detection systems for AI-generated abuse including deepfakes and synthetic content
- **Performance-based compliance** scoring for platform accountability addressing current enforcement crisis

#### **Graduated Accountability System:**

- **12-hour acknowledgment** requirement for all TFGBV reports submitted to platforms
- **24-hour initial decision by platforms** with clear explanation of policies and reasonings
- **Warnings and penalties for compliance failures** - fines for repeated non-compliance
- **Mandatory Annual Compliance Reports** from each platform operating in Pakistan
- **Regular audits of platform TFGBV** response capabilities of platforms

#### **Addressing Global Standards vs Local Law Conflicts:**

- **Diplomatic initiatives** with platform headquarters countries for recognition of Pakistani legal standards
- **Bilateral cooperation frameworks** addressing current MLAT gaps
- **Regional coalition building** with South Asian and Muslim-majority countries for collective platform accountability
- **International advocacy for Global South perspectives** in platform governance frameworks

### **E) Social Response**

#### **Community and Cultural Change:**

- **Community awareness campaigns challenging victim-blaming culture** that characterises Pakistan's response to TFGBV
- **Develop all public awareness materials in accessible formats** including captions, audio descriptions, and plain language versions

- **Behaviour Change Communication targeting generational gaps** in attitudes and behaviours
- **Public education on digital rights and reporting mechanisms** through multiple channels
- **Influencer and celebrity engagement for youth outreach** leveraging social media reach
- **Family and peer group interventions for attitude change** addressing cultural factors

## 7

## ADDRESSING EMERGING TECHNOLOGY CHALLENGES

Technology-facilitated gender-based violence continues to evolve faster than existing legal and institutional responses. New forms of digital abuse including AI-generated content, deepfakes, and sophisticated synthetic media disproportionately target women, while current platform limitations and detection challenges create significant gaps in protection. This strategy outlines a response that addresses the emerging technological threats while building resilient protection mechanisms.

### 7.1. AI-Generated Content Crisis

**The Challenge:** Deepfakes, AI-generated hate content, and sophisticated fake accounts are escalating faster than platform detection systems can manage. 95% of deepfake sexually explicit content is of women, representing an acute threat to women's digital safety in Pakistan.

#### Current Status:

- 1.5 million complaints received by PTA, with only 100,000 addressed
- Increase in defamation, impersonation, and indecent content specifically targeting women and other vulnerable communities
- No gender-disaggregated data tracking of cases - PTA and NCCIA

#### Strategic Response:

- **Improved forensics of Deepfake for prosecution** with specialised technical capabilities to detect AI generated content
- **Platforms based AI systems specifically trained to identify TFGBV content patterns, with regular auditing, bias testing, and cultural context training** to detect harassment campaigns before they escalate
- **Bias testing for Human Supervised AI-assisted case classification and chatbot systems** ensuring equitable treatment across diverse communication styles and behaviours
- **Cross-border cooperation for transnational digital crimes** addressing jurisdictional challenges

- **Contextualised responses based on local considerations** recognizing cultural factors in implementation.

## 7.2. Understanding Perpetrator Behaviour - MMO Framework

### Motivation, Means, and Opportunity (MMO) Analysis:

- **MOTIVATION:** Intent to harm (misogyny, revenge, control)
- **MEANS:** Access to tools (fake accounts, spyware, personal data)
- **OPPORTUNITY:** Gaps in monitoring, weak laws, anonymity

### Prevention Through "Target Hardening":

- **Motivation + Means, No Opportunity:** Strong platform security prevents action
- **Means + Opportunity, No Motivation:** Tools exist but no intent - crime unlikely
- **Motivation + Opportunity, No Means:** Intent exists but lacks tools - crime blocked

**Focus:** Preventive efforts on limiting opportunity through better platform safeguards, user privacy education, and stronger institutional protocols.

### Regulatory Framework: Addressing the Platform Enforcement Crisis

**The Challenge:** Current platform cooperation rates create an enforcement lottery where identical TFGBV acts receive vastly different responses based solely on corporate policies rather than legal merits or harm severity:

- Meta (Facebook/Instagram/WhatsApp): 75% compliance with Pakistani data requests
- X (Twitter): ~0% compliance since 2021 (creating digital sanctuary for perpetrators)
- TikTok: 16.3% compliance for legal requests

This platform lottery system means justice depends on which platform perpetrators choose rather than the severity of harm or clarity of domestic law, creating widespread impunity for TFGBV.

**Strategic SMPRA Implementation for TFGBV:** The new regulatory framework offers unprecedented opportunities to address this enforcement crisis through:

- Mandatory 24-hour content removal addressing viral spread of intimate images
- Platform compliance requirements ending voluntary cooperation model
- Emergency BSI sharing protocols for high-risk TFGBV cases
- Graduated penalties from warnings to complete platform blocking

**Critical Implementation Requirements:**

- Clear jurisdictional division preventing survivors from being shuttled between Authority, Council and NCCIA
- TFGBV-specific expertise within regulatory structure
- Fast-track procedures for emergency cases involving threats of offline violence
- Appeal mechanisms accessible to ordinary litigants (not requiring Supreme Court proceedings)

**Addressing Global Standards vs Pakistani Law Conflicts:**

- Regulatory requirements for platforms to recognize Pakistani legal standards in TFGBV cases
- Mandatory context-specific community guidelines reflecting local cultural and legal frameworks
- International diplomatic engagement for Global South perspectives in platform governance
- Regional coalition building for collective platform accountability

The transformation from reactive content removal to proactive platform accountability could fundamentally alter Pakistan's response to TFGBV. Success depends on implementation that prioritizes survivor needs and justice delivery over technical compliance, ensuring that regulatory power translates into meaningful protection for women across all digital platforms.

## 8 IMPLEMENTATION FRAMEWORK

The framework establishes governance structures, coordination mechanisms, and implementation phases designed to ensure systematic rollout across Pakistan's complex federal-provincial system. The framework emphasizes accountability, stakeholder integration, and evidence-based monitoring to deliver measurable improvements in Pakistan's response to TFGBV.

### Universal Accessibility

The strategy mandates that All TFGBV response systems, including reporting mechanisms, helplines, mobile applications, court facilities, digital evidence handling platforms, and support services, must be designed with universal accessibility as a mandatory requirement, ensuring barrier-free access for women and girls with disabilities. Accessibility measures shall be compliant with WCAG 2.1 AA standards for digital systems, sign language interpretation services, accessible physical infrastructure, plain language communication, and assistive technology compatibility.

### 8.1. Governance Structure

#### National TFGBV Coordination Cell

**Location:** Ministry of Human Rights

#### Functions:

- Facilitate coordination between federal and provincial authorities for consistent TFGBV response
- Establish permanent inter-ministerial working groups linking Ministry of IT, Law & Justice, Interior, and relevant Commissions and stakeholders including relevant institutions and departments
- Maintain dedicated civil society advisory positions ensuring survivor-centred approaches
- Develop comprehensive international cooperation protocols for cross-border digital crimes
- Monitor implementation progress against baseline statistics

- Ensure integration with existing treaty reporting mechanisms for CEDAW compliance

### Inter-Ministerial Working Groups

#### Core Participating Ministries:

- Ministry of Information Technology (platform regulation and technical cooperation)
- Ministry of Law & Justice (legal framework reforms and judicial coordination)
- Ministry of Interior (law enforcement coordination and security aspects)
- Ministry of Commerce (international trade and platform negotiations)

#### Supporting Institutions:

- National Commission for Human Rights (NCHR)
- National Commission on Status of Women (NCSW)
- National Commission on Rights of Child (NCRC)
- National Police Bureau (NPB)
- Federal Ombudsman for Protection of Harassment of Women at Workplace (FOSPAH)
- PKCERT

## 8.2. Integrated Support Systems

#### Key Helplines Integration:

- **1099:** MoHR Helpline for Human Rights (now has dedicated GBV tele-app tracking TFGBV cases)
- **15:** Police Helpline – Virtual Women Police Station (integration with local response capabilities)
- **1799:** NCCIA (specialized cybercrime response with technical capabilities)
- **NCSW** helpline – in the process of being established

#### Support System Components:

- Link Police 15, MoHR's 1099 helpline, NCSW helpline with 1799 NCCIA for comprehensive 24/7 support

- **NCCIA online reporting portal and app with NADRA verification** to remove in-person verification requirement
- **AI-powered support systems, with human supervision:** Deploy Sara-style AI chatbots providing 24/7 anonymous legal advice, safety planning, and resource navigation with multilingual support
- **Human Supervised AI-assisted classification to prioritize cases based on severity, risk factors, and urgency indicators** ensuring high-risk cases involving threats of honor-based violence receive immediate attention within 2-4 hours
- **Psychosocial support and access to female staff** across all service points
- **Inter-agency referral and response protocols** ensuring streamlined case transfer and management

#### Reporting Infrastructure Improvements:

- **Updated PTA and NCCIA websites** explaining reporting processes and options
- **Clear guidance for reporting to both authorities** with user-friendly interfaces
  - **User-friendly interfaces adapted for Pakistani context** with local and regional language support

#### Emergency Response Capabilities:

- **Platform emergency coordination** for suicide threats and imminent harm
- **24-hour platform response capability** for high-risk situations
- **Prioritized case handling for high-risk situations** using complaint classification system

### 8.3. Implementation Strategy

#### Legislative Reforms and Foundation Building (Immediate - 6 months)

##### Legislative Priority Actions:

- **Define TFGBV in the law** providing all-encompassing legal definition of the offences
- **Strengthen procedural law** to enable effective prosecution of TFGBV offences

- **Implement mandatory platform data-sharing provisions** for high-risk cases

#### **Institutional Foundations:**

- **Establish National TFGBV Coordination Cell** within MoHR with dedicated staffing
- **Parliamentary engagement through Women Parliamentary Caucus** sessions with structured presentations
- **Provincial assembly consultations** across all four provinces for federal-provincial coordination
- **National assembly consultation** for legislative support and awareness

#### **PPPR Rollout and Service Delivery (06-12 months)**

##### **Response Implementation:**

- **Establish decentralized service delivery** through SDPO-level cybercrime units
- **Launch prevention and education programs** including HEC curriculum integration
- **Deploy survivor support services** with intersectional approach
- **Digital case management system implementation within NCCIA** with complaint classification

##### **Capacity Building:**

- **Expand NCCIA personnel** with focus on female officer recruitment
- **Technology infrastructure upgrades** for secure digital evidence handling
- **Training programs** for law enforcement, prosecutors, and judicial authorities

#### **Platform Response and International Cooperation (12-24 months)**

##### **Regulatory Framework:**

- **Full operationalisation of SMPRA, Council, and Tribunals** with TFGBV-specific protocols

- **Address jurisdictional ambiguities** through detailed implementation guidelines
- **Establish clear appeal procedures** preventing survivor re-victimization
- **Implement graduated platform accountability system** with enforcement mechanisms

#### **Platform Accountability:**

- **Implement platform compliance protocols** with graduated penalty system
- **Address enforcement crisis** through mandatory cooperation frameworks
- **Establish international cooperation frameworks** for transnational cases
- **Deploy AI detection systems** for deepfakes and TFGBV as mandatory platform requirement for operations in Pakistan
- **Regular audits of platform TFGBV response** through mandated bi-annual performance sharing

#### **Transnational Cooperation:**

- **Cross-border enforcement** through mutual legal assistance treaties
- **Bilateral agreements** with platform headquarters jurisdictions
- **Regional cooperation frameworks** for cross-border TFGBV cases
- **Diplomatic engagement for Global South perspectives** on international platforms

## 9

## MONITORING AND EVALUATION FRAMEWORK

The monitoring and evaluation framework establishes a mechanism for tracking progress, measuring impact, and ensuring accountability in TFGBV strategy implementation. It defines performance indicators aligned with baseline statistics, establishes monitoring mechanisms for continuous improvement, and integrates evaluation findings into management processes. The framework ensures that Pakistan's response evolves based on evidence and remains responsive to changing technological and social contexts.

### 9.1. Performance Indicators and Baseline Metrics

#### Current Baseline Statistics (2024):

- **65% of complaints** achieve no meaningful legal outcome
- **1.2% success rate** – complaint redressal by NCCIA (1,664 out of 135,000 complaints)
- **Platform compliance variations:** 0% X (Twitter), 75% Meta, 16.3% TikTok
- **900+ complaints per NCCIA officer** annually with Rs. 9,000 monthly budget
- **428 FIRs registered** for gender-based violence under PECA amendments by NCCIA

#### Performance Tracking Mechanisms:

- **Monitoring timelines to track conversion rates** from TFGBV complaints to prosecutions across the relevant agencies and departments
- **Clear timelines and milestones** for each intervention outlined in the four pillars

#### Success Targets (2-year goals):

- Increase prosecution success rate to at least 15% in TFGBV cases
- Reduce response times for critical priority cases to under 24 hours
- Achieve minimum 50% platform compliance with data requests across all platforms
- Establish 100+ SDPO-level cybercrime units nationwide
- Reduce cases with no meaningful outcome from 65% to under 20% - for TFGBV cases

## INTERSECTIONAL APPROACHES AND VULNERABLE POPULATIONS

Special population groups and implementation considerations require tailored approaches within the broader PPPR framework. These specialised focus areas emphasize intersectional vulnerabilities including disability, transgender identity, linguistic minorities, and economic disadvantage that compound TFGBV risks. The strategy ensures an inclusive approach that recognises how multiple forms of marginalization intersect to heighten TFGBV risks.

**Disability Inclusion:** Embedding disability inclusion from the outset is critical, starting with the definition and overall strategy. Women and girls with disabilities are more vulnerable, especially in online contexts, requiring:

- **Special protections** for persons with disabilities in all PPPR pillars
- **Training for on-ground staff** to respond to specific needs of persons with disabilities
- **Safe and accessible reporting and support mechanisms** designed with disability considerations
- **Accessible technology interfaces** for reporting

**Transgender Community Support:**

- **Specialised support for transgender community** addressing unique vulnerabilities
- **Targeted measures for transgender persons** in protection and response mechanisms
- **Inclusive training programs** for law enforcement and support staff
- **Recognition of intersectional vulnerabilities** in service delivery

**Linguistic Diversity:**

- Addressing Pakistan's diverse linguistic landscape, the reporting mechanisms, support services, and awareness materials will be made available in Urdu, Pashto, Sindhi, Punjabi, and Balochi to ensure universal accessibility across all provinces

## 11

## RISK MANAGEMENT AND MITIGATION STRATEGIES

The strategy recognises potential challenges to effective implementation and establishes proactive mitigation approaches to ensure resilient and adaptive TFGBV response. It addresses political, institutional, resource, and social risks that could undermine implementation success while providing concrete mitigation strategies. The framework enables responsive course correction and continuous improvement based on emerging challenges and lessons learned during implementation.

### 11.1. Implementation Challenges and Mitigation

#### Political and Institutional Risks:

- **Risk:** Lack of sustained political commitment across government changes
- **Mitigation:** Embed strategy in treaty obligations and constitutional frameworks, ensure cross-party support through parliamentary engagement

#### Resource and Capacity Constraints:

- **Risk:** Insufficient funding for comprehensive implementation
- **Mitigation:** Phased implementation approach, international cooperation for technical assistance, evidence-based advocacy for budget increases

#### Platform Non-Cooperation:

- **Risk:** Continued platform resistance to compliance requirements
- **Mitigation:** Graduated penalty system, international cooperation frameworks, regional coordination

#### Cultural and Social Resistance:

- **Risk:** Victim-blaming culture undermining reporting and support seeking
- **Mitigation:** Behaviour change communication through awareness programmes, community engagement, influencer partnerships for cultural change

## 11.2. Monitoring and Course Correction

### Adaptive Implementation Framework:

- **Regular strategy review cycles** incorporating lessons learned and emerging challenges
- **Stakeholder feedback mechanisms** ensuring continuous improvement based on ground realities
- **Performance indicator adjustments** responding to changing technological and social contexts

## 12 CONCLUSION AND CALL TO ACTION

Pakistan stands at a critical juncture in addressing tech-facilitated gender-based violence. This comprehensive PPPR strategy provides a roadmap for transformation from crisis management to comprehensive protection, but success requires collective commitment from all stakeholders. The framework establishes immediate next steps, accountability mechanisms, and a shared vision for Pakistan's digital future where every citizen can participate safely and fully in the country's digital transformation.

### The Path Forward Requires Collective Commitment:

- **Government:** Political will, resource allocation, inter-agency coordination, and sustained implementation across political cycles
- **Civil Society:** Advocacy, survivor support, Disabled persons Organisations, monitoring implementation
- **Private Sector:** Platform cooperation, technology solutions, compliance with regulatory requirements, and corporate social responsibility for digital safety
- **International Partners:** Technical assistance, capacity building, cooperation in cross-border cases, and support for Pakistan's treaty compliance efforts
- **Communities:** Cultural change supporting survivors, challenging victim-blaming attitudes, and creating enabling environments for women's digital participation

## National Strategy for Addressing TFGBV 2026-2030

### Strategic Actions Implementation Table

#### PILLAR 1: PREVENTION

Sr	Action	Timeline	Responsibility
1	Develop and integrate mandatory 3 credit-hour TFGBV module in HEC curriculum across all academic disciplines	Immediate - 6 months	HEC, Universities
2	Launch nationwide Behaviour Change Communication (BCC) campaign targeting toxic masculinity and victim-blaming culture	3-6 months	MoHR, MoIT&T, NCSW
3	Engage religious leaders, community elders, lady health workers for promoting women's digital rights	6-12 months	MoRA, NCSW, Civil Society
4	Implement public awareness campaigns using SMS, short videos, and community sessions	6-12 months	PTA, MoIT&T, NCCIA
5	Establish Safety by Design protocols with automated detection systems for platforms	6-12 months	SMPRA, PTA, MoIT&T
6	Deploy AI tools for myth-busting and fact-checking on social media platforms	12-18 months	SMPRA, Platform Companies
7	Establish Digital Safety Resource Centres in universities, schools, colleges and community centers	12-18 months	HEC, Provincial Governments

#### PILLAR 2: PROTECTION

Sr	Action	Timeline	Responsibility
8	Operationalize SMPRA's 24-hour content removal mandate for TFGBV cases	Immediate - 3 months	SMPRA, Mol
9	Establish emergency protocols for online-to-offline violence escalation	Immediate - 3 months	NCCIA, Provincial Police, Mol
10	Integrate 24/7 helplines (1099, 15, 1799) for comprehensive TFGBV response	3-6 months	MoHR, NCCIA, Provincial Police

11	Draft standardized case transfer guidelines for technology facilitated crimes, defining clear criteria for transfer from local police stations to NCCIA from SMPRA and the Council	6-12 months	National Police Bureau, NCCIA, Provincial Police, SMPRA
12	Develop survivor-centric support services with legal aid and counselling	6-12 months	MoHR, NCSW, Provincial Social Welfare
13	Create dedicated TFGBV reporting channels within Social Media Complaint Council	6-12 months	Social Media Complaint Council, SMPRA
14	Establish SDPO-level cybercrime units with trained staff	6-12 months	Provincial Police, NCCIA
15	Implement trauma informed court procedures with video link, and disabled persons compatible communication options	12-18 months	Ministry of Law & Justice, Judiciary
16	Deploy multilingual support systems for linguistic minorities	12-18 months	MoHR, NCSW, Provincial Governments
17	Strengthen print and electronic media regulations to prohibit the dissemination and publication of technology-facilitated gender-based violence content	12-18 months	PEMRA, Ministry of Human Rights, District Human Rights Committees

### PILLAR 3: PROSECUTION

Sr	Action	Timeline	Responsibility
18	Legislate to define TFGBV in the law - outlining the contours of the crime in clear terms and the types of associated offences	Immediate - 90 days	Ministry of Law & Justice, Parliament
19	Strengthen procedural law to enable effective prosecution of TFGBV offences	Immediate - 6 months	Ministry of Law & Justice, Parliament
20	Implement Digital Case Management System with Human Supervised AI-assisted classification	3-6 months	NCCIA, MoIT&T
21	Expand NCCIA personnel to 2500+ officers with focus on female recruitment	6-12 months	NCCIA, Ministry of Interior
22	Increase investigation budget for TFGBV cases	6 months	NCCIA
23	Establish specialized TFGBV prosecution units within NCCIA	6-12 months	NCCIA, Prosecutor General

24	Implement mandatory platform data-sharing provisions	12-18 months	SMPRA, Ministry of Law & Justice
25	Deploy technological upgrades for secure digital evidence handling	12-18 months	NCCIA, PKCERT
26	Introduce professional trainings on TFGBV for Police, Prosecution and Judges	12-18 months	Ministry of Law & Justice, Ministry of Interior

#### PILLAR 4: RESPONSE

Sr	Action	Timeline	Responsibility
27	Establish National TFGBV Coordination Cell under the supervision of MoHR	Immediate - 90 days	MoHR, NCSW
28	Implement emergency 24-hour BSI sharing protocols for high-risk cases	Immediate - 3 months	SMPRA, Platform Companies
29	Establish 2-hour acknowledgment requirement for TFGBV platform reports	3 months	SMPRA, Platform Companies
30	Develop sentencing guidelines with defined adjudication timelines	6-12 months	Supreme Court, Ministry of Law & Justice
31	Create inter-ministerial working groups for policy alignment	6 months	MoHR, MoIT&T, MoL&J, Ministry of Interior
32	Implement graduated platform accountability system with compliance scoring and mandate publication of annual reports	12-18 months	SMPRA, MoIT&T
33	Establish bilateral cooperation frameworks with platform headquarters countries	12-24 months	Ministry of Foreign Affairs, MoIT&T
34	Improve enquiry conducting capacity of NCSW, PCSWs	12-24 months	MoHR, NCSW, PCSWs

### EMERGING TECHNOLOGY & AI CHALLENGES

Sr	Action	Timeline	Responsibility
35	Develop improved forensics capabilities for deepfake detection and prosecution	6-12 months	NCCIA
36	Mandate platform deployment of AI systems trained to identify TFGBV patterns	12-18 months	SMRA, Platform Companies
37	Establish cross-border cooperation for transnational digital crimes	12-24 months	Ministry of Foreign Affairs, NCCIA

### INSTITUTIONAL CAPACITY BUILDING

Sr	Action	Timeline	Responsibility
38	Continue Technical Working Group sessions at MoHR with expanded participation	Immediate - Ongoing	MoHR
39	Launch pilot SDPO-level cybercrime units in major metropolitan areas	90 days - 6 months	Provincial Police, NCCIA
40	Train prosecutors on digital evidence and trauma-informed approaches	6-12 months	Prosecutor General, NCCIA
41	Establish specialized TFGBV benches within existing courts	6-12 months	High Courts, Sessions Courts
42	Achieve gender-balanced recruitment (30:70 ratio) in TFGBV units	24 months	NCCIA, Provincial Police

### MONITORING & EVALUATION

Sr	Action	Timeline	Responsibility
43	Establish baseline data collection with gender-disaggregated statistics	Immediate - 3 months	NCCIA, PTA, NCSW
44	Develop performance indicators tracking prosecution success rates	6 months	National TFGBV Coordination Cell
45	Integrate TFGBV data with CEDAW treaty reporting mechanisms	6-12 months	MoHR, NCSW
46	Conduct annual platform compliance audits and publish reports	12 months onwards	SMPRA, National TFGBV Coordination Cell

### VULNERABLE POPULATIONS & INTERSECTIONALITY

Sr	Action	Timeline	Responsibility
47	Develop disability-inclusive reporting and support mechanisms, Awareness Campaigns	6-12 months	MoHR, NCSW, CSOs
48	Create specialized support services for transgender community	6-12 months	MoHR, NCSW, Trans Rights Organizations

### INTERNATIONAL COOPERATION

Sr	Action	Timeline	Responsibility
49	Initiate Mutual Legal Assistance Treaties for cross-border evidence collection	6-12 months	Ministry of Foreign Affairs, MoL&J
50	Build regional coalition for platform accountability	12-24 months	Ministry of Foreign Affairs, MoIT&T
51	Advocate for Global South perspectives in international platform governance	24-36 months	Ministry of Foreign Affairs, MoIT&T

### LONG-TERM SUSTAINABILITY

Sr	Action	Timeline	Responsibility
52	Achieve reduction in TFGBV incidents through effective deterrence	5 years	National TFGBV Coordination Cell, All Stakeholders
53	Increase women's social media usage from 47% to 75%	5 years	MoIT&T, NCSW, Platform Companies
54	Improve Pakistan's women's access to justice score from 1.53 to 2.5	5 years	Ministry of Law & Justice, Judiciary
55	Establish Pakistan as regional best practice model for TFGBV response	5 years	MoHR, Ministry of Foreign Affairs



**United Nations Development Programme**

4th Floor, Serena Business Complex,  
Khayaban-e-Suharwardy, G-5/1, Islamabad, Pakistan  
[www.pk.undp.org](http://www.pk.undp.org)



[/UNDPPakistan](https://www.facebook.com/UNDPPakistan)



[/UNDP\\_Pakistan](https://twitter.com/UNDP_Pakistan)



[/UNDP\\_Pakistan](https://www.instagram.com/UNDP_Pakistan)



[/UNDPPakistan](https://www.linkedin.com/company/undp-pakistan)



MINISTRY OF HUMAN RIGHTS  
GOVERNMENT OF PAKISTAN

**Ministry of Human Rights, Government of Pakistan**

9th Floor, New Pak Secretariat (Kohsar Block)  
Sector F-5, Islamabad  
[www.mohr.gov.pk](http://www.mohr.gov.pk)



[@mohrpakistan](https://www.facebook.com/mohrpakistan)



[@mohrpakistan](https://twitter.com/mohrpakistan)