UK International Development
Partnership | Progress | Prosperity

Awaz اواز

LAS
LEGAL AID SOCIETY

UNFPA
The United Nations sexual and reproductive health agency

Technology-Facilitated Gender-Based Violence in Pakistan:

CRITICAL GAPS IN JUSTICE SYSTEM'S RESPONSE

Technology- Facilitated Gender- Based Violence in Pakistan

CRITICAL GAPS IN JUSTICE SYSTEM'S RESPONSE

Technology-Facilitated Gender-Based Violence in Pakistan: Critical Gaps in the Justice System's Response

Year of Publication: 2025

For more copies and other related queries, please contact:

Legal Aid Society
1st Floor, Block C, FTC Building, Shahra-e-Faisal, Karachi, 75350
Tel: +92-21-35634112 | +92-21-35634113
Email: hr@lao.org.pk, info@lao.org.pk
Website: https://www.las.org.pk
Facebook: Legal Aid Society Pakistan

Legal Aid Society is registered under the Societies Registration Act, 1860, on November 19, 2013 (Registration No. KAR 058 of 2013–14) and operates under the chairpersonship of Justice Nasir Aslam Zahid, former Judge of the Supreme Court of Pakistan and former Chief Justice of Sindh High Court.

Acknowledgments

UNFPA Pakistan and Legal Aid Society (LAS), acknowledges the contributions of all stakeholders who supported the development of the report Technology-Facilitated Gender-Based Violence in Pakistan: Critical Gaps in the Justice System's Response. We thank government representatives, law enforcement officials, legal experts, civil society partners, and team members whose insights and efforts were essential to the completion of this publication.

We would also like to thank the Foreign, Commonwealth & Development Office (FCDO) for their generous support, without which this research would not have been possible. We are also thankful to the Legal Aid Society for their technical insights for developing this research study.

Core Team

Author: **Amna Baig**
Research Support: **Haleema Hijazi**

Advisory & Technical Support

Advocate Maliha Zia Lari (Director Gender, Inclusion & Development, Legal Aid Society)
Dilshad Pari (Gender & GBV Analyst)

Citation

About the Authors

Author: Amna Baig

Amna Baig is a Superintendent of Police in the Pakistan Police Service and a leading policy expert on gender-based violence. She established Pakistan's first Gender Protection Unit and currently leads the development of Pakistan's National Framework on Tech-Facilitated Gender-Based Violence. At the University of Oxford's Blavatnik School of Government, she conducted research on technology-facilitated violence against women (TFVAW) and has since advised on strategic international initiatives including the National Democratic Institute's rapid response mechanism for women facing digital violence and pirth.org, a trust and safety platform for reporting online threats. She has presented on TFGBV at the UN Forums, the United States Institute of Peace, and the Aspen Institute. Amna is a Yale World Fellow, an Eisenhower Fellow, and holds a Master of Public Policy from the University of Oxford and a Bachelor of Laws from the University of London.

Assisted by: Haleema Hijazi

Haleema Hijazi is a postgraduate student reading for a Master’s degree in Modern South Asian Studies at the University of Oxford. She has previously worked as a Research Assistant in the Department of Law at SOAS University of London.
Haleema Hijazi is a postgraduate student reading for a Master’s degree in Modern South Asian Studies at the University of Oxford. She has previously worked as a Research Assistant in the Department of Law at SOAS University of London.

Table of Content

Message from

Dr. Luay Shabaneh

Country Representative, UNFPA

The rapid growth of digital technologies in Pakistan has transformed communication, access to information, and civic engagement. However, alongside these opportunities, new forms of violence against women and girls have emerged. Technology-facilitated gender-based violence (TFGBV) is an increasingly pervasive threat that undermines human rights, gender equality, and access to justice, with repercussions that extend well beyond the digital realm.

Pakistan's existing legal and institutional frameworks have not kept pace with this evolving digital landscape. Survivors of TFGBV face numerous obstacles in seeking justice, including mandatory in-person verification procedures. Law enforcement and regulatory authorities often lack the specialized training, resources, and operational mechanisms necessary to prevent or respond effectively to these crimes. These gaps perpetuate impunity and exacerbate offline violence, psychological, physical, social, and economic, that limit women's participation in public, political, and economic life.

This report provides a comprehensive analysis of these challenges, combining quantitative data and qualitative insights within Pakistan's legal, social, and cultural context. It offers survivor-centered recommendations aimed at strengthening the justice system and regulatory framework. Key proposals include establishing specialized TFGBV units within the National Cybercrime Investigation Agency, introducing digital reporting mechanisms, enacting TFGBV-specific legislation, conducting awareness and prevention campaigns, and ensuring timely, context-sensitive responses from social media platforms.

Aligned with Pakistan's obligations under international frameworks—including the UN Sustainable Development Goals 5 and 16, and CEDAW General Recommendations 19 and 35—this report underscores that addressing TFGBV is both a national priority and a matter of social equity. Implementing these recommendations can make digital spaces safer and more inclusive, reinforce gender equality, and ensure access to justice for women and girls.

Comprehensive action against TFGBV will not only protect individuals online but also strengthen the broader social fabric, enabling women to participate fully and safely in all spheres of public, social, and economic life. The government of Pakistan is strongly encouraged to hold technology providers accountable for safety measures and ensure that perpetrators are brought to justice. Addressing TFGBV is a crucial accelerator of women's empowerment and a key driver for Pakistan's future prosperity.

Message from

Haya Emaan Zahid

Chief Executive Officer, Legal Aid Society

Technology-facilitated gender-based violence has become one of the most pervasive threats to women's safety, agency, and participation in public life. While digital spaces offer opportunity, they have also expanded the reach of harassment, coercion, and exploitation. This study exposes the systemic gaps in our current response landscape, including limitations within the Prevention of Electronic Crimes Act, the lack of recognition for threats made prior to content disclosure, and the absence of legal safeguards for online intimate-partner violence.

Through our work, we see every day how systemic gaps delay protection and restrict access to justice for survivors. Legal Aid Society has been contributing by providing legal assistance, supporting strategic litigation, and building the capacity of police and prosecution on gender-based violence laws.The insights gathered from police, prosecution, and cybercrime officials highlight a clear mandate: Pakistan needs a faster, more adaptive, and survivor-centered legal and institutional framework to address TFGBV. Our commitment is to strengthen partnerships with state institutions, development actors, and communities to ensure that every woman and girl can meaningfully and safely claim her digital rights.

EXECUTIVE SUMMARY

KEY FINDINGS AT A GLANCE

- Pakistan's legal framework inadequately addresses evolving types and spectrum of technology-facilitated gender-based violence (TFGBV)
- Law enforcement and regulatory bodies lack specialized training and resources for prevention and response to TFGBV
- Survivors face significant barriers to justice including mandatory in-person verification requirements for processing legal complaints
- Widespread impunity exists due to systemic failures across institutions and laws

This report examines critical gaps in Pakistan's justice system in addressing technology-facilitated gender-based violence (TFGBV) and provides recommendations based on contextual realities of South Asia and global best practices. The analysis combines a qualitative literature review with quantitative data on TFGBV cases and institutional responses.

Within the framework of UN Sustainable Development Goal 5 (Gender Equality) and SDG 16 (Peace, Justice and Strong Institutions), the report highlights how TFGBV undermines both gender equality and access to justice in Pakistan. The findings align with CEDAW General Recommendations 35 on gender-based violence and General Recommendation 19 on violence against women. The findings and recommendations are highly relevant to Global South countries, particularly those with similar legal systems, cultural contexts, and platform accountability challenges.

The Problem
Pakistan's current legal framework does not comprehensively address evolving forms of TFGBV. Law enforcement, regulatory authorities and judicial institutions lack the specialized capacity and resources needed for effective redressal of TFGBV. Survivors face significant barriers to justice, including mandatory in-person verification requirements to have complaints registered with the designated investigation agency that often prevent them from seeking legal recourse, even in severe cases of TFGBV.

The Consequences
The consequences extend far beyond digital harassment. TFGBV creates lasting offline harm including physical and psychological violence, social isolation, and economic exclusion that forces many women to withdraw from online spaces and civic participation, resulting in a chilling effect. This perpetuates a cycle where the limited response from the justice system enables continued abuse and restrict women's broader socio-political and economic engagement.

The Data Gap

Widespread underreporting, driven by cultural stigma and institutional barriers, means available data likely underrepresents the problem's true scope[1]. Despite these limitations, consistent patterns across multiple sources confirm both the prevalence of TFGBV and systemic failures in addressing it, contributing to massive impunity for perpetrators.

The Solution
The report presents survivor-centred recommendations targeting immediate legal reforms and capacity improvements across criminal justice and regulatory institutions. Key recommendations include establishing specialized TFGBV units within the National Cybercrime Investigation Agency (NCCIA), implementing digital reporting mechanisms, developing TFGBV-specific legislation tailored to Pakistan's legal framework and cultural context, advancing prevention through comprehensive awareness campaigns, and advocating on international forums for contextualized regulations and swift responses by social media platforms to cases and data requests by local regulatory bodies.

[1]Amna Baig, "Securing Democracy: Enhancing Digital Protection for Women Politicians in Pakistan" (Blavatnik School of Government, University of Oxford, 2024) https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf.

2012

5 girls murdered in Kohistan after video went viral

2016

Naila Rind commited suicide after digital blackmail

2016

Qandeel Baloch killed by brother for social meida presence

Today

Thousands of women and girls face similar risk across Pakistan

INTRODUCTION

In 2012, five girls were murdered in the Kohistan region of Pakistan after a video of them singing and clapping went viral. The video was widely circulated throughout the region via Bluetooth, ultimately leading to the honour killing of those who appeared in what seemed like a harmless act of celebration[2]. Naila Rind, a student from Sindh province, committed suicide following exploitation and blackmail over private digital photographs by a man[3]. Qandeel Baloch, a rising social media influencer, was killed by her own brother for her career choices[4]. Today, thousands of girls and women across Pakistan, where deeply entrenched patriarchal attitudes already limit women's public and private autonomy, face the risk of serious violence that is either facilitated, amplified, or directly perpetrated through technology in today's digital world[5].

[2]https://www.washingtonpost.com/world/in-pakistan-five-girls-were-killed-for-having-fun-then-the-story-took-an-even-darker-twist/2016/12/16/f2adbd5e-c13a-11e6-92e8-c07f4f671da4_story.html
[3]https://www.dawn.com/news/1374502
[4]https://www.bbc.com/news/world-asia-49874994
[5]https://digitalrightsfoundation.pk/subject-over-20000-cases-of-technology-facilitated-gender-based-violence-tfgbv-received-by-digital-rights-foundations-helpline-during-8-years-of-operation/

1.1 What is TFGBV?

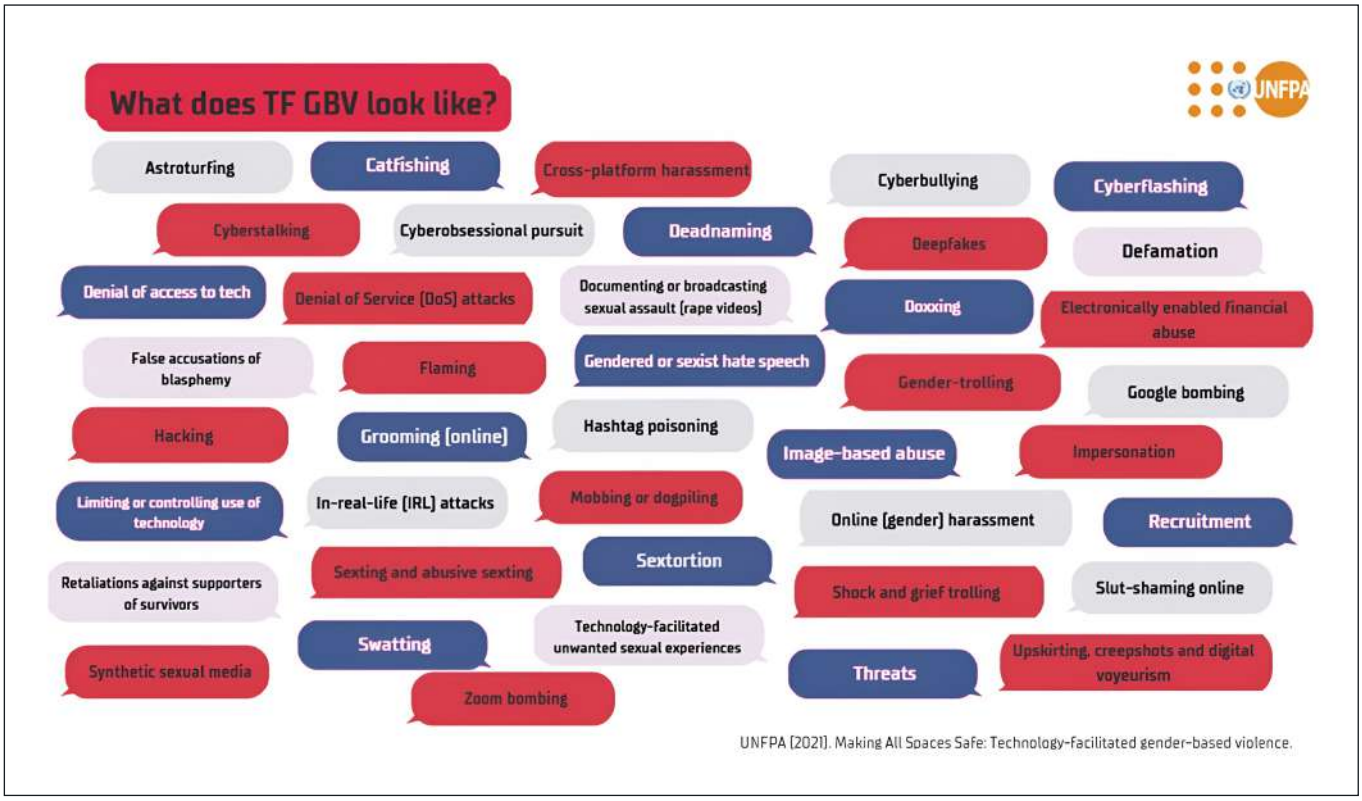
The abovementioned cases exemplify a broader phenomenon known as Tech-Facilitated Gender-Based Violence (TFGBV). TFGBV, as defined by the UN Special Rapporteur, encompasses:

any act of gender-based violence against women that is committed, assisted or aggravated by the use of Information and Communication Technology, impacting them disproportionately[6].

The United Nations Population Fund (UNFPA) defines it as:
"an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender[7]*."*.

In simpler terms, TFGBV comprises any act that leverages technology, digital tools, or digital platforms, whether social media, messaging apps, or AI, to inflict, facilitate, or amplify harm against women, including physical, sexual, and psychological violence, thereby curtailing their fundamental rights and freedoms.

Some key manifestations of TFGBV include[8]:
- Doxxing (publishing private information)
- Cyber harassment
- Online blackmail and threats
- Image-based abuse
- Cyber stalking
- Misogynistic hate speech
- Impersonation
- Sextortion (sexual extortion)[9]



The consequences of TFGBV are devastating for Pakistani women, ranging from social ostracization and mental health trauma to honour-based violence and, in extreme cases, femicide. In deeply patriarchal contexts, where women's digital and physical autonomy are widely contested, TFGBV becomes a mechanism to silence, shame, and exclude women from public life. This is not an unintended consequence of digital innovation; rather, it represents the manifestation of entrenched gendered power imbalances that have found new expression through modern tools and platforms.

TFGBV is not a side effect of technology, it is a deliberate tool of patriarchal control that has found new digital expression.

[6]ttps://documents.un.org/doc/undoc/gen/g18/184/58/pdf/g1818458.pdf?OpenElement
[7]UNFPA, 2021 "Technology-facilitated Gender-based Violence: Making All Spaces Safe"
[8]https://www.unfpa.org/TFGBV
[9]https://www.unfpa.org/sites/default/files/pub-pdf/An%20Infographic%20Guide%20to%20An%20Infographic%20Guide%20to%20TFGBV.pdf

The resulting marginalization undermines women's access to the evolving technological ecosystems. In today's interconnected world, digital engagement is essential for full participation in modern life, from education and healthcare to employment, financial services, civic engagement, and creative expression. Yet the threat of TFGBV, combined with existing structural barriers including limited access to devices, gendered restrictions on mobility, and inadequate digital literacy support, continues to exclude millions of Pakistani women and girls from this vital space.

The stakes of addressing TFGBV thus extend beyond individual safety to fundamental questions of equality, participation and empowerment. Given these circumstances, there is an urgent need for examination of Pakistan's justice sector response to TFGBV, particularly how legal and regulatory frameworks, law enforcement capabilities, and judicial processes address these evolving forms of technology-facilitated gender-based violence.

1.2 Understanding TFGBV in Its Two Distinct Forms

Since violence is associated with tangible, visible consequences, understanding TFGBV requires recognizing its two distinct forms: direct TFGBV and structural TFGBV.

Direct TFGBV is relatively straightforward to identify. It includes overtly harmful acts such as: image-based abuse, blackmail, cyber stalking, sextortion, doxxing, etc. These are attacks where there is a clear perpetrator targeting a specific victim with malicious intent.

Structural TFGBV is more complex and harder to identify. It operates through widespread patterns of behaviour that make digital spaces hostile to women. This might include: constant sexist harassment, gender-based trolling, misogynistic comments, and coordinated abuse campaigns.

Female politicians are 27 times more likely to face online abuse than their male counterparts (Amnesty International)[10]

These patterns of behaviour, while often not illegal, disproportionately affect women. Collectively, these patterns extend beyond individual victims to create an environment where women feel unwelcome or unsafe on social media platforms, effectively limiting their participation in digital public discourse.

At its core, direct TFGBV involves attacks on individuals that are categorized as criminal under legal definitions, whereas structural TFGBV creates broader systemic conditions that discourage women's digital participation. While these forms operate through different mechanisms, they frequently reinforce one another, limiting women's full engagement in the digital sphere.

Correspondingly, their redressal pathways differ significantly. Direct TFGBV is primarily addressed through the criminal justice system, whereas structural TFGBV is dealt with through regulatory frameworks and platform-based reporting mechanisms.

[10]https://www.uk-cpa.org/news-and-views/online-violence-against-women-parliamentarians-hinders-democracy-and-all-parliamentarians-are-responsible-for-addressing-it

METHODOLOGY

This research uses a mixed approach using qualitative and quantitative analysis to examine TFGBV in Pakistan, combining desk-based review, publicly available data, expert interviews, and practitioner insights with a survivor-centric approach.

2.1 Data Collection Methods

The study relies on three key sources:

i. Desk Review

Analysis of relevant laws, policies, judicial decisions, departmental reports, publicly available data, and academic literature on TFGBV and cybercrime in Pakistan, focusing particularly on:

- Prevention of Electronic Crimes Act (PECA) and its amendments
- Pakistan Penal Code relevant provisions
- Judicial decisions and departmental reports

ii. Key Informant Interviews

Semi-structured interviews conducted between March-July 2025 with senior personnel from Federal Investigation Agency's former Cyber Crime Wing, National Cyber Crime Investigation Agency officials, officials who have investigated TFGBV cases, lawyers specializing in cybercrime, women's rights activists, and survivors of TFGBV.

iii. Practitioner Insight and Positionality:

The author's direct supervision of investigations into gender-based violence and TFGBV cases provides an embedded, insider perspective that enriches the analysis. This dual position—as both researcher and practitioner—offers access to internal processes, investigative patterns, and survivor experiences that are rarely documented in formal data.

2.2 Limitations

Data gaps: Official statistics do not provide gender-disaggregated cybercrime figures or distinguish technology-facilitated gender-based violence (TFGBV) from general cybercrime and complaint categories, thereby limiting quantitative analysis.

Underreporting: TFGBV remains significantly underreported due to stigma and lack of trust and awareness about the reporting mechanisms within the justice system.

Technological evolution: The rapid pace of digital change has outstripped legal reform and institutional capacity.

Despite these limitations, the study offers a comprehensive analysis of TFGBV in Pakistan, grounded in institutional insight and survivor-centred perspectives. The findings will guide targeted policy recommendations for strengthening Pakistan's justice sector response to TFGBV.

2.3 The Research Question

Addressing TFGBV requires comprehensive legal, institutional, and social safeguards that enable women, girls, and other vulnerable groups to engage in digital spaces safely. This research examines how TFGBV manifests in Pakistan as both individual acts of digital violence and a structural tool of gendered control that penalizes women for their digital visibility.

The central question guiding this analysis is: *How does TFGBV operate in Pakistan, and what challenges within the legal, regulatory, and digital ecosystems contribute to its persistence and ensuing impunity?*

By situating TFGBV within the lived realities of Pakistani women, whether digitally present or not, the study underscores that the harms extend beyond technology to encompass social, political, legal, and institutional dimensions. The chapters ahead examine the patterns, challenges and limitations that characterize Pakistan's current response to TFGBV and identify pathways toward redressal and accountability.

DECODING TFGBV IN PAKISTAN: THE GENDERED DIGITAL CONTEXT

Pakistan has 240 million people navigating an increasingly digital world. Nearly half are women, with 93 million under the age of 40[11]. While digital access is expanding rapidly, 08 million women went online in 2024 alone, significant inequalities persist that create vulnerabilities to technology-facilitated violence[12]. A striking 35% of women who use mobile internet do not own their device and depend on borrowing phones[13].

PAKISTAN'S DIGITAL LANDSCAPE

- 240 million total population
- 93 million women under age 40
- 8 million women came online in 2024 alone
- 35% of women don't own their internet device

[11]https://moib.gov.pk/News/62983
[12]https://www.pta.gov.pk/category/mobile-internet-adoption-2024-1073985202-2025-05-20
[13]Ibid

3.1 The Gender Digital Divide

ALARMING GAP
Male social media usage: 78%
Female social media usage: 47%
Most TFGBV perpetrators are men = Higher risk environment for women

When social media statistics are analysed from a gendered perspective, these disparities become even more concerning. Male social media usage stands at 78% while female usage remains at only 47%[14]. Since the perpetrators of TFGBV are most commonly men[15], this substantial gender gap creates an environment where women are at a higher risk of encountering digital abuse. Moreover, women's reliance on shared devices further compromises their control and privacy over online presence and digital safety.

3.2 Evidencing the Gap: Case Studies

i. Political Targeting

2024 ELECTION DATA		
117 gendered disinformation cases identified	84 cases (72%) targeted women specifically	53%+ involved false claims about personal lives

According to data collected in a study during the election period in 2024 in Pakistan, political leaders received the highest volume of gendered disinformation posts, with women being the primary targets in 84 out of 117 identified cases[16]. In the documented cases of TFGBV during the 2024 elections, women politicians were singled out with manipulated content; much of it focused on, personal attacks, false claims about private life and use of AI-altered media to cause harm17. These campaigns sought to damage credibility and discourage public participation among female candidates.

This content often combined[18]:

- False claims about their personal lives (found in over 53% of submissions)
- Manipulated media (including AI-generated images)
- Attacks on professional credibility

Such digital campaigns are a prime example of gendered disinformation, a form of TFGBV that uses misleading or false content to reinforce patriarchal control and punish women for their visibility. Women in public roles, especially politicians, journalists, influencers, human rights defenders, and those in the entertainment industry, are disproportionately targeted. These orchestrated attacks seek to discredit women leaders and isolate them from support networks. They silence women through fear, forcing self-censorship. The overall effect is a systematic silencing of women's voices in the digital public sphere, creating what scholars call the *chilling effect*.

ii. Female Journalists Under Digital Attack

Women journalists in Pakistan have in particular borne the brunt of this aggression. A study conducted in 2019 surveying women in the media and information sectors, found:

55% of women in media experienced online abuse, only 14.2% sought assistance resulting in a massive gap between harm and help-seeking[19]

An escalation was evidenced in the lead-up to the 2024 general elections in Pakistan, with targeted narratives aimed at delegitimizing female journalists, and activists becoming more frequent and technologically sophisticated[20]. An unprecedented wave of online attacks was directed at female journalists covering political developments on mainstream platforms and sharing commentary on social media during the said elections[21].

High-profile female journalists were subjected to[22]:

- Gendered slurs, coordinated harassment campaigns
- Circulation of doctored images and deepfake videos
- Non-consensual leakage of personal photographs and information

These attacks intensified after journalists criticized major political parties, resulting in organized retaliation by partisan supporters[23]. The uniformity of language, timing of posts, and use of coordinated hashtags, often from recently created or dormant accounts, pointed to deliberate, strategic attempts to silence female voices.

[14]https://www.pta.gov.pk/assets/media/pta_ann_rep_2022_gender_mainstreaming_ict_10-05-2024.pdf
[15]https://www.unfpa.org/sites/default/files/pub-pdf/An%20Infographic%20Guide%20to%20An%20Infographic%20Guide%20to%20TFGBV.pdf
[16]Digital Rights Foundation, Gendered Disinformation During Elections in Pakistan (Lahore: Digital Rights Foundation, March 2025), https://digitalrightsfoundation.pk/wp-content/uploads/2025/03/Gendered-Disinformation-During-Elections-in-Pakistan.pdf.
[17]Digital Rights Foundation, Gendered Disinformation in South Asia Case Study – Pakistan (Digital Rights Foundation, 2024), https://digitalrightsfoundation.pk/wp-content/uploads/2024/10/DRF-Case-Study-GD-SA.pdf.
[18]Ibid
[19]Digital Rights Foundation, Fostering Open Spaces in Pakistan: Combatting Threats to Women's Activism Online (Digital Rights Foundation, 2019), https://digitalrightsfoundation.pk/wp-content/uploads/2019/04/IMS-Study-Report.pdf.
[20]Digital Rights Foundation, Gendered Disinformation in South Asia Case Study – Pakistan (Digital Rights Foundation, 2024), https://digitalrightsfoundation.pk/wp-content/uploads/2024/10/DRF-Case-Study-GD-SA.pdf.
[21]Ibid
[22]Ibid
[23]Ibid

PATTERN OF COORDINATED ATTACKS	
• Uniformity of language across attacks • Synchronized timing of posts	• Coordinated hashtag campaigns • Recently created or dormant accounts

This behavioural pattern highlights not only unequal access, but also the limited control and autonomy women have over their digital presence.

3.3 The Restrictive Response

In Pakistan, the predominant response to TFGBV involves limiting women's access to technology and digital spaces, whether imposed by families and communities or adopted by survivors as self-preservation and protection. However, such approaches do not address the root causes while further marginalizing women from essential digital participation and associated educational and employment opportunities.

Aspect	Details
Problem	Technology-facilitated gender-based violence (TFGBV) threatens women online
Common Response	Limiting women's digital access to digital spaces
Result	Further marginalization, with root causes left

When women are pressured to censor themselves online or minimize their digital presence, the consequences extend far beyond the internet. This self-restriction limits their access to information, professional networks, educational resources, and civic participation opportunities.

More troubling, this restrictive approach normalizes the expectation that women should protect themselves by withdrawing from digital spaces. Families, communities, and institutions begin to view such self-censorship as the appropriate response to online harassment. This not only leads to a culture of victim-blaming where women who maintain their online presence are seen as inviting abuse, but also enables continued impunity for the perpetrators of TFGBV.

LEGAL FRAMEWORK ANALYSIS

KEY TERMS FOR THIS SECTION

- **PECA:** Prevention of Electronic Crimes Act (Pakistan's main cyber law)
- **CEDAW:** Convention on Elimination of Discrimination Against Women
- **SMPs:** Social Media Platforms

Since Pakistan is a signatory to (Convention on the Elimination of All Forms of Discrimination Against Women), it is mandated to adopt criminalization of all forms of GBV against women without exemptions. While the Pakistan Penal Code 1860 contains the majority of provisions relating to criminal law, Pakistan enacted a special law to address online harms: the Prevention of Electronic Crimes Act (PECA) 2016.

4.1 The Governing Law – PECA 2016, 2023, 2025

PECA Timelines

2016	2023	2025
Originak act (designed to address cyber harassment of women)	Find Amendment	SecondAmendment

Problem: Neither amendment specifically addresses TFGBV

The PECA Act 2016 creates jurisdiction over criminal complaints of TFGBV. Originally designed to address cyber harassment of women, it has not achieved this goal despite two amendments within a short span of eight years[24].

More concerning is the fact that while complaints of TFGBV have risen exponentially[25], neither amendment addresses the issue in specific terms nor mentions offenses against women. Instead, the law has increasingly gained a reputation as an instrument for curtailing dissent. The limitations become more apparent when specific provisions that could potentially address TFGBV cases are reviewed. A fundamental gap is the Act's reliance on vague and overly broad terminology such as "dishonest," "dissemination of information," and "hatred" which fails to provides the legal clarity required for effective prosecution of TFGBV offenses.

4.2 PECA: Three Key Sections for TFGBV

The criminal redressal of TFGBV complaints relies on the following three key sections of PECA that NCCIA frequently invokes for investigative purposes:

4.2.1 Section 20: Offences Against Dignity of a Natural Person

Section 20: Offences against dignity of a natural person

(1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

OVERVIEW OF SECTION 20

- Purpose: Criminalizes public display/transmission of false and harmful information
- Usage: Most frequently used for TFGBV complaints
- Problem: Focuses on dissemination, does not address threats of dissemination or violence

Section 20 criminalizes the intentional public display or transmission of false information that intimidates or harms the reputation of a natural person, making it the provision most frequently used by the NCCIA to register TFGBV complaints. Despite this widespread application, the section has a fundamental flaw in that it focuses on the dissemination of offensive content rather than addressing the technology-facilitated nature of these crimes.

The narrow focus on dissemination is reflected in the legal terminology, which creates significant gaps in protection. Content must be *"exhibited," "displayed publicly,"* or *"transmitted"* to constitute a criminal offense. This means the law does not address instances where perpetrators create or record objectionable content and threaten to share such content without publishing it.

CRITICAL GAP
Threats to disseminate intimate content is **not covered by Section 20**, yet threat itself causes serious psychological harm and coercion

Such threats constitute a common form of technology-facilitated blackmail where the threat itself needs to be considered the crime.

[24-25]https://digitalrightsfoundation.pk/subject-over-20000-cases-of-technology-facilitated-gender-based-violence-tfgbv-received-by-digital-rights-foundations-helpline-during-8-years-of-operation/

The Vagueness Paradox

Equally problematic, the section's broad and undefined terms such as "intimidates" and "privacy" result in legal challenges due to their vagueness. Without definitions, these are defined as per the discretion of the investigators or the judges with no consistency, resulting in a major loophole: behaviour that one court may treat as criminal intimidation, another may dismiss as harmless online speech. Further, these terms do not comprehensively capture the essence of TFGBV as they are too general to capture the specific harms women face online e.g. blackmail to release intimate pictures or repeated anonymous harassment, while also creating tensions with freedom of expression. The said definitional shortcomings reflect the Act's limited acknowledgement of the nuanced ways technology facilitates violence against vulnerable populations.

Non-Cooperation by Social Media Platforms

ENFORCEMENT REALITY
Even when TFGBV complaints filed → Social media platforms refuse data sharing → Investigations stall → Rarely convert to FIRs → No prosecutable cases → Impunity

More critically, the section's effectiveness is severely curtailed by social media platforms' (SMPs) limited data sharing with the NCCIA. The lack of cooperation by SMPs brings investigations to a standstill, specifically in cases of anonymous perpetrators. When complaints are filed against perpetrators hiding behind anonymous accounts, the NCCIA requires basic subscriber information (BSI) from SMPs to track their identities. However, the platforms often refuse to share the required data, which means such cases are rarely prosecuted due to the inability of the LEA to identify the accused[26].

4.2.2 Section 16: Unauthorized Use of Identity Information

Section 16: Unauthorized use of identity information.

(1) Whoever obtains, sells, possesses,transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both

(2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information

OVERVIEW OF SECTION 16
- Purpose: Prohibits using another person's identity information
- Covers: Impersonation, fake profiles, doxxing
- Status: Non-cognizable offense (requires court order to investigate)
- Issues: Vagueness + Platform non-cooperation

The enforcement challenges are not unique to Section 20. Section 16 demonstrates the same pattern of legal shortcomings. This section prohibits obtaining, selling, possessing, transmitting, or using another person's identity information. It addresses cases of impersonation through fake profiles used for doxing and disseminating sensitive personal information. While this section targets a critical form of TFGBV, it exhibits the same vagueness issue that undermines the entire Act.

The broad legal language lacks specificity and measures of severity. The generic categorization treats even grave technology-facilitated crimes as non-cognizable offenses. Victims of serious TFGBV find their complaints conflated with less severe violations, undermining the legal system's overall response to gender-based digital violence. The section's inability to distinguish between varying levels of harm illustrates how the Act's vague terminology creates practical enforcement issues.

Double Barrier to Justice

PROCEDURAL NIGHTMARE
Non-cognizable status = Court order required for investigation + Platform data refusal = Investigation Blocks = Women left without legal recourse

Section 16 faces the dual challenge of procedural delays and data unavailability from social media platforms. The non-cognizable status requires court orders for investigation, often prolonging the process by adding additional layers in investigation. Meanwhile, platforms frequently decline requests for crucial identification data by NCCIA. Consequently, complaints rarely progress to registration of a case, leaving women without meaningful legal recourse against identity-based online abuse.

[26]Hannah Phillips and Rosario Grimà Algora, eds., Strengthening Democracy by Reducing Threats to Women in Politics: Local Evidence, Shared Solutions Compendium Report (Oxford: Blavatnik School of Government, University of Oxford, 2024), https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf.

4.2.3 Section 21: Offences Against Modesty of a Natural Person

Section 21: Offences against modesty of a natural person and minor.

(1) Whoever intentionally and publicly exhibits or displays or transmits any information which:

(a)superimposes a photograph of the face of a natural person over any sexually explicit image or video; or

(b)includes a photograph or a video of a natural person in sexually explicit conduct; or

(c)intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or

(d)cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both

(2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees:
Provided that in case of a person who has been previously convicted of an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.

(3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

OVERVIEW OF SECTION 21

- Purpose: Criminalizes sexually explicit content sharing
- Relevance: 95% of AI-generated sexual content depicts women
- Covers: Intimate image abuse, deepfakes, non-consensual sharing
- Status: Cognisable and Non-compoundable (victims cannot settle with accused)

The enforcement challenges become even more pronounced with Section 21, which addresses the most severe forms of TFGBV. This section criminalizes the public exhibition, display, or transmission of sexually explicit content, including intimate image abuse. The section has gained particular relevance with the emergence of AI-generated deepfake content, specifically since 95% of sexually explicit generative AI content depicts women[27]. It deals with complaints involving sexually explicit photos and sharing of non-consensual private photos and other objectionable content that not only damages a person's reputation but often triggers severe offline repercussions[28].

Section 21 demonstrates clarity in defining offense parameters compared to other sections. However, its efficacy is also affected by the blackmail loophole discussed earlier. Instances where criminal content exists and is used to threaten but has not been made "public" or "transmitted", fall outside the section's scope.

THE THREAT PROBLEM
Possessing intimate images + threatening to share = Serious psychological harm + Coercion
But not "public" or "transmitted" yet = Outside the scope of Section 21

This creates significant gaps in protection as the threat of publication constitutes serious psychological harm and coercion for victims, regardless of whether content is published.

Section 21 is subject to mostly the same challenges discussed above. Despite being non-compoundable (meaning victims cannot settle with accused parties), the lengthy legal procedures often result in informal compromises outside the court system. Most critically, limited data sharing by social media platforms continues to obstruct case registration against anonymous perpetrators of this particular form of TFGBV.

[27]https://giwps.georgetown.edu/resource/technology-facilitated-gender-based-violence/
[28]https://edition.cnn.com/2020/05/18/asia/pakistan-honor-killing-hnk-intl

REGULATORY FRAMEWORK:

The Pakistan Telecommunication Authority (PTA), The Social Media Regulatory Authority, Council and Tribunal

- **KEY TERMS FOR THIS SECTION**
- **PTA:** Pakistan Telecommunication Authority (current regulator)
- **SMRA:** Social Media Protection and Regulatory Authority (new body)
- **PECA 2025:** Latest amendment creating new regulatory structure

5.1 Original Framework: PTA

PTA 2024

- 1.5 million complaints received
- ~100,000 addressed
- Notable increase in gender-based content cases
- No gender-disaggregated data available

The Pakistan Telecommunication Authority (PTA), operating under PECA 2016 and mandated to regulate social media platforms, received over 1.5 million complaints and addressed around 100,000 in 2024, with officials noting a noticeable increase in cases of defamation, impersonation, and gender-based harassment.

However, as a regulatory body, PTA's role remained limited to forwarding received complaints to social media platforms. The evaluation of harmful content then relies on platforms' global community standards, which often do not account for the specific context of TFGBV in Pakistan.

5.2 The Current Framework: PECA Amendment 2025

The PECA Amendment 2025 introduces a new regulatory framework that will replace PTA upon establishment. While concerns remain regarding independence and other institutional shortcomings, this new framework offers potentially improved pathways for addressing TFGBV.

Specifically, the amendments establish a three-tier complaint review system for cyber issues, as following:

Social Media Protection and Regulatory Authority (SMRA): The SMRA serves as the primary regulatory body with extensive powers including, content regulation, blocking/removal orders, and/or platform enlistment[29].

The Council: The Council serves as a complaints processing body responsible for receiving and acting on public complaints of PECA violations.

The Tribunals: The Tribunals represent the appellate tier, hearing appeals against Authority decisions. Importantly, appeals against Tribunal decisions would go directly to the Supreme Court, bypassing High Courts and potentially creating access barriers for ordinary litigants who may find Supreme Court proceedings prohibitively expensive and complex.
Although these bodies have been officially notified, they are yet to be established and operationalised.

5.2.1 Limitations of the Current Regulatory Framework

JURISDICTIONAL CONFUSION

Problem: Act doesn't clarify which complaints go to Authority vs Council
Risk: TFGBV victims shuttled between institutions while harmful content spreads

The Amendment 2025 does not clarify which complaints would go to the Authority versus the Council, despite both bodies being mandated with complaint-handling. This jurisdictional ambiguity is further complicated by the lack of clarity regarding which matters should be criminally investigated by the NCCIA, the premier law enforcement agency for handling cybercrimes. This jurisdictional confusion could prove particularly detrimental for TFGBV victims, who may be shuttled between institutions while harmful content continues to spread unchecked, causing persistent psychological trauma and threats of physical harm.

The lack of role clarity also creates accountability gaps: when a case stalls, no single institution can be held responsible for inaction. It also undermines data collection, as complaints are dispersed across agencies with no centralized registry.

5.2.2 Promising Features

POTENTIAL IMPROVEMENTS

- 24-hour content removal mandate
- Specialized TFGBV reporting channels possible
- Platform compliance requirements
- Rapid administrative process vs lengthy criminal procedures

Despite these structural flaws, the framework addresses critical timing dimensions of TFGBV harm. The SMRA's mandate to issue removal/blocking orders within 24 hours under Section 2C could provide immediate relief for TFGBV victims, directly countering the current system's inability to timely prevent viral distribution of intimate images or harassment content. The capacity to respond rapidly addresses the most urgent gap in existing enforcement mechanisms, where platforms prioritize engagement over safety and complaint procedures offer limited relief.

The Council's design offers a promising avenue for survivor-centred TFGBV response, despite the jurisdictional ambiguities. It could establish dedicated TFGBV reporting channels with trained female

[29]https://rsilpak.org/2025/2025-amendments-to-the-prevention-of-electronic-crimes-act-2016-an-introduction/

personnel who understand the contextual realities and unique challenges women face, including fear of further victimization and social stigma that prevents them from seeking help. This specialized approach could potentially address the under-reporting crisis that characterizes TFGBV cases in Pakistan.

The Authority's power to regulate platforms and impose compliance requirements could require social media companies to implement stronger TFGBV prevention measures, automated detection systems, and contextualised user protection protocols. Rather than navigating complex criminal procedures that often result in no meaningful relief, victims could access a specialized administrative process designed for rapid content removal with platform accountability with penalties being imposed accordingly.

Although this institutional framework has certain limitations, it creates infrastructure that could considerably improve TFGBV responses if implemented with gender-sensitive protocols. However, realizing the framework's potential for TFGBV protection will require implementation that consistently prioritizes victim safety and support.

IMPLEMENTATION CHALLENGES

6.1 The Implementing Agency: From FIA to NCCIA

INSTITUTIONAL TRANSITION
FIA Cyber Crime Wing → National Cyber Crime Investigation Agency (NCCIA)
Problem: New agency inherits same resource constraints and barriers

PECA 2025 replaced the Federal Investigation Agency's Cyber Crime Wing with the National Cyber Crime Investigation Agency (NCCIA). This transition was intended to signal a stronger, more specialized state response to the rapidly growing challenge of cybercrime, including TFGBV. In theory, a standalone agency with dedicated jurisdiction represents an opportunity to streamline operations, build technical expertise, and improve responsiveness to victims. However, the new agency inherits the same resource constraints, geographic limitations, and procedural barriers that rendered its predecessor ineffective in comprehensively addressing TFGBV.

6.2 Process of Filing Complaints

It is important to outline the process for handling cybercrime complaints currently in place at NCCIA. Complaints can be registered through multiple channels: the online portal, a helpline (which is frequently non-functional), email, or in-person visits to cyber police stations. Following registration, complaints undergo a verification process that requires complainants to visit cybercrime police stations in person. Once verified, a formal enquiry is conducted into the matter. If substantial evidence of cybercrime exists, a First Information Report is registered, and the investigation begins. This process typically takes:

- **1-2 weeks** for cases involving known perpetrators
- **2-3 months** for cases with anonymous perpetrators (as data requests must be sent to social media platforms for Basic Subscriber Information (BSI))

CURRENT COMPLAINT PROCESS

1. Report via: Online portal / helpline / email / in-person
2. Verification: Mandatory in-person visit to cyber station
3. Enquiry: Formal investigation (1-2 weeks for known perpetrators/2-3 months anonymous perpetrators)
4. FIR: Case registration (if sufficient evidence is found)
5. Investigation: Begins after FIR registration

6.3 Challenges for the NCCIA

6.3.1 Geographic Centralization – Limited Access to Justice

The 2025 Amendment removes all provincial police jurisdiction, requiring that "only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act." With only 15 cybercrime police stations across Pakistan, NCCIA cannot meaningfully serve 240 million people. The mandatory in-person verification requirement further limits access to justice for TFGBV complainants, particularly women. This reflects Pakistan's broader struggles with providing survivor-centered justice services to women within accessible geographic range. Pakistan ranks 1.53 on a scale of 4 for this measure, among the lowest globally[30].

Geographical Centralization - Limited Access to Justice

Cultural restrictions on women's mobility, family opposition, victim blaming and economic limitations already prevent many TFGBV survivors from seeking help. The legal requirement of physical presence at cybercrime police stations for complaint verification compounds the issue, particularly given the vast geographic distances involved.

Balochistan: A Case Study in Inaccessibility

The issue is particularly stark in Balochistan, Pakistan's largest province by area, which has only two cybercrime police stations serving its entire territory. In case a woman in Turbat experiences intimate image-based abuse, she would have to travel over 150 kilometres to reach the nearest cybercrime

[30]https://giwps.georgetown.edu/country/pakistan/

police station in Gwadar. According to 2024 data, Gwadar cybercrime police station recorded zero conversions from enquiries to registered cases, a statistic that likely reflects geographic inaccessibility rather than absence of digital violence[31].

6.3.2 Jurisdictional Limbo

The 2025 amendment complicates the status of existing cases registered with provincial police departments. The 2023 amendment had granted limited powers to provincial police for verification and case registration under PECA before transferring investigations to the FIA. However, many cases registered by provincial police under this framework remained under local investigation rather than being transferred as mandated by the law.

Following the 2025 amendment's complete removal of provincial police authority on the subject matter, these cases now exist in a jurisdictional limbo. Without a formal transfer mechanism between the law enforcement agencies, TFGBV complainants whose cases were registered with provincial police find their investigations trapped between institutions, with unclear authority for continuation or completion[32].

6.3.3 Human and Material Resource Constraints

i. Impossible Caseload

2024 NCCIA PERFORMANCE GAP

- 135,000 complaints received nationwide
- 46,649 converted to enquiries (34%)
- 1,664 registered as cases/FIRs (1.2%)
- 826 proceeded to prosecution (0.6%)
- 65% achieved NO meaningful legal outcome

The 2024 Cyber Crime Wing annual report shows that out of the average of 135,000[33] complaints received nationwide, 46,649[34] were converted into enquiries, and only 1,664[35] were formally registered as FIRs. Only 826[36] cases proceeded to prosecution, whereas 65% of complaints achieved no meaningful legal outcome. Such a sharp attrition rate reflects not only procedural bottlenecks but also the chronic human and resource constraints that the agency faces in managing the exponential growth of cybercrime.

For online harassment specifically, the FIA Cyber Crime Wing registered only 459 cases (FIRs) and made 437[37] arrests in 2024. However, these available official figures do not reflect the true scale and prevalence of tech-facilitated gender-based violence in Pakistan. While disaggregated official data on TFGBV complaints submitted to cybercrime police stations remains unavailable, independent sources reveal an alarming situation.

The Digital Rights Foundation's Cyber Harassment Helpline, a non-profit initiative, handled over 20,000 cases of digital violation from 2016-2024. They received 3,171 new cases in 2024 alone, out of which 1,794 were online harassment complaints, including:

- 1,772 from women
- 18 from transgender persons
- 4 from non-binary individuals[38]

This represents nearly four times the number of cases formally registered by the FIA[39]. The figures highlight a significant gap between reported incidents and official case registration that suggests substantial under-reporting or weak institutional response to TFGBV complaints within the formal justice system.

RESOURCE REALITY

~200 investigation officers across 15 stations
135,000 complaints annually
= 900+ complaints per officer per year
+ 35,218 pending enquiries creating years-long backlogs
+ Only 7 prosecutors nationwide for concluded investigations

Despite these established procedures, fundamental human resource limitations severely compromise their effectiveness. Approximately 200[40] investigation officers handle caseloads of around 135,000 complaints across 15 stations, with each officer processing an average over 900 complaints annually. The resulting 35,218 pending enquiries[41] create an impossible backlog that stretches investigation timelines for years. With only seven prosecutors at NCCIA, delays persist nationwide even after investigations conclude.

ii. Financial Architecture of Neglect

Officers receive Rs. 9,000 (USD 32) monthly for all investigation related activities, approximately Rs. 1,080 per complaint[42]. This amount cannot cover basic verification procedures, let alone the complex investigations required for sophisticated digital crimes involving multiple platforms, anonymous accounts, or AI-generated content.

[31]https://fia.gov.pk/files/publications/431604082.pdf
[32]https://tribune.com.pk/story/2452941/islamabad-police-empowered-to-probe-cybercrimes
[33]Federal Investigation Agency, Head Quarters, 2024
[34]https://www.fia.gov.pk/files/tickers/165919683.pdf?utm_source=perplexity
[35] https://fia.gov.pk/files/publications/431604082.pdf
[36]Ibid
[37]https://fia.gov.pk/files/publications/431604082.pdf
[38]https://digitalrightsfoundation.pk/wp-content/uploads/2025/04/Digital-Security-Helpline-Annual-Report-2024-1.pdf
[39]https://fia.gov.pk/files/publications/431604082.pdf
[40]Federal Investigation Agency, Head Quarters, 2024
[41]https://www.fia.gov.pk/files/tickers/165919683.pdf?utm_source=perplexity
[42]https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf

iii. Expertise Cannot Develop in Volume-Processing System

TFGBV cases require understanding digital platforms, gender dynamics, technological manipulation, ever-changing technological advancements, and how online abuse translates into offline violence. A specialized expertise cannot develop within a system designed for processing a huge volume of cases and neither can such a system offer the sensitive and dedicated case handling and management that TFGBV cases demand.

iv. Infrastructure Limitations Create Additional Risks

The inadequate funding extends to basic infrastructure and evidence handling capabilities. Most cybercrime police stations operate from rented buildings with inadequate seating arrangements for investigation officers, creating an environment unsuitable for handling confidential digital evidence that demands privacy and secure processing.

EVIDENCE SECURITY CRISIS

- Minimal evidence storage capabilities
- No proper SOPs for sensitive digital data
- Risk of intimate image/communication leakage
- No secure transfer protocols to forensic labs

= Investigation process itself becomes potential source of harm

Evidence storage capabilities at NCCIA remain minimal due to these logistical and resource constraints, compromising not only the integrity of digital evidence crucial for TFGBV prosecutions, but also creating risks of mishandling and data leakage. The substandard conditions undermine the credibility of investigations and potentially jeopardize cases before they reach the prosecution stage.

More critically, the system lacks proper standard operating procedures for handling sensitive digital data, particularly intimate images and personal communications central to TFGBV cases. Without established protocols for secure transfer to forensic laboratories, digital evidence faces significant risks of leakage or misuse—a devastating prospect for survivors whose intimate content could be further weaponized against them. This procedural gap renders the investigation process itself into a potential source of additional harm for TFGBV victims.

SOCIAL MEDIA PLATFORMS: THE DIGITAL ENFORCEMENT CRISIS

THE PROBLEM
Pakistani authorities can investigate and prosecute tech crimes
but effectiveness depends entirely on platforms' voluntary cooperation which leads to
Enforcement failures and widespread impunity for anonymous perpetrators

Pakistan's criminal justice response to TFGBV faces a critical gap: social media platforms operating beyond the reach of domestic law enforcement. While Pakistani authorities investigate and prosecute technology-facilitated crimes, their effectiveness depends entirely on platforms' voluntary cooperation, a dependency that has created enforcement failures and enabled widespread impunity for anonymous perpetrators.

7.1 Limited Data Sharing

THE ENFORCEMENT LOTTERY
Meta (FB / Instagram / WhatsApp): 75% compliance
TikTok: 16.3% compliance
X/Twitter: 0% compliance
Justice depends on which platform perpetrators choose

The investigation of TFGBV cases relies on social media platforms sharing Basic Subscriber Information (BSI) to identify anonymous perpetrators, and other account data for verification purposes. However, compliance and response rates vary dramatically across platforms, creating an arbitrary system where justice depends on which platform offenders choose.

Women Politicians: A Case Study
This is evident in Pakistan's case of 25 TFGBV complaints by women politicians since 2018, 21 involving unknown accounts. Most anonymous complaints failed to convert into prosecutable investigations, with only 4 cases proceeding to prosecution, 3 involving known perpetrators and 01 where authorities identified the accused through Pakistan's national identity database[43]. The lack of cooperation for anonymous cases is compounded by platforms' practice of holding public figures to higher standards for harassment claims, creating additional barriers specifically for women politicians seeking justice.

7.2 Platform-by-Platform Analysis

i. Meta: The Cooperative Exception

The platform-by-platform analysis reveals the extent of this enforcement lottery. Meta demonstrates a 75% compliance rate with data requests from NCCIA, enabling authorities to identify accused in cybercrime cases involving Facebook, Instagram, and WhatsApp[44]. This cooperation stems from established relationships between Meta and the country's law enforcement, built through years of structured engagement and investigators gaining experience in submitting well documented requests.

ii. X/Twitter: The Digital Perpetrator's Sanctuary

X/TWITTER: COMPLETE NON-COOPERATION

- Zero compliance with Pakistani data requests since 2021
- 17 information requests (July-Dec 2021) = 0 responses
- 4 emergency requests = 0 responses
- Creates digital sanctuary for TFGBV perpetrators

In stark contrast, X (formerly Twitter) maintains virtually zero compliance with data requests from Pakistan's Law Enforcement Agencies since 2021[45]. Pakistani authorities made 17 information requests during July-December 2021 alone, including 4 emergency requests, yet received zero responses. This deliberate non-cooperation creates a digital sanctuary for TFGBV perpetrators who understand that using X essentially guarantees anonymity and impunity, no matter how serious their acts are.

i. TikTok: Selective Responsiveness

TIKTOK: MIDDLE GROUND WITH BUSINESS PRIORITIES

- 16.3% compliance for legal data requests (Jan-June 2024)
- 113 total requests: 86 legal + 22 emergencies
- Only 13.6% compliance for emergency requests responds to content removal in 3 days causeing letting business priorities override criminal justice needs

TikTok occupies middle ground with 16.3% compliance for legal data requests during January-June 2024, though the platform responds more readily to content removal demands[46]. Pakistani authorities made 113 total requests during this period, including 86 legal requests and 22 emergency requests, yet secured data in fewer than 1 in 6 cases, and only 13.6% for emergency requests[47]. This selective responsiveness exemplifies how platform business priorities override criminal justice needs. While TikTok responds to content concerns within days, requests from law enforcement agencies face delays and frequent denials. The Digital Rights Foundation reported TikTok resolved cases through escalation in just three days[48], yet this responsiveness reflects content removal rather than the sharing of BSI which is necessary for criminal prosecution, effectively shielding TFGBV perpetrators.

KEY INSIGHT
The highlighted disparities create an enforcement landscape where identical criminal acts encounter vastly different outcomes based solely on corporate policies rather than legal merits or harm severity.

[43]https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf
[44]https://transparency.meta.com/reports/government-data-%20requests/country/PK/
[45]https://transparency.x.com/en/reports/countries/pk
[46]https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf
[47]https://www.tiktok.com/transparency/en/information-requests-2024-1
[48]https://digitalrightsfoundation.pk/wp-content/uploads/2025/04/Digital-Security-Helpline-Annual-Report-2024-1.pdf

7.3 Limited Data Sharing

THE DISCONNECT
Pakistani law: Section 21 criminalizes sexually explicit content sharing
Platform Response: Apply global standards with higher thresholds
Result: Refusal or unresponsiveness to BSI requests for cases that are serious crimes under domestic law

These disparate compliance rates reflect a deeper structural conflict between global platform policies and domestic criminal justice requirements. Section 21 of PECA criminalizes sharing of sexually explicit content based on local cultural standards, recognizing that such material can have devastating offline repercussions for women in Pakistan. Yet platforms apply global community guidelines with higher thresholds, refusing to provide BSI data for cases that constitute serious crimes under domestic law.

7.3.1 Global North Bias in Platform Governance

REPRESENTATION PROBLEM
Platform standards shaped by: Global North regulatory/legal/cultural norms
Missing: Global South perspectives, especially South Asian voices
Result: Standards overlook context-specific harms in countries such as Pakistan

This disconnect reflects a broader structural issue: the limited representation of Global South perspectives, particularly from South Asia, in the development of platform governance frameworks. Community standards, content moderation protocols, and data disclosure policies are predominantly shaped by regulatory, legal, and cultural norms from the Global North. While these global standards aim to maintain consistency across jurisdictions, they can inadvertently overlook or inadequately respond to context-specific harms experienced in countries like Pakistan. The lack of engagement with local stakeholders, including governments, civil society, and digital rights advocates, contributes to this misalignment.

In practice, platforms may decline to provide BSI in cases that, while not violating global standards, clearly constitute crimes under domestic law. Without this basic subscriber information, authorities cannot provide legal redress for victims of contextualized TFGBV, specifically in cases of anonymous perpetrators. This violence often escalates rapidly to severe offline harms, including honour-based violence, forced marriage, physical assault, and femicide.

MUTUAL LEGAL ASSISTANCE TREATY (MLAT)
Pakistan lacks MLATs with countries hosting major platforms
- Meta: Declines 25% of Pakistani requests citing MLAT absence
- X: Uses this justification to refuse virtually ALL cooperation

The absence of Mutual Legal Assistance Treaties (MLATs) between Pakistan and countries hosting major platforms deepens the aforementioned challenges. Platforms frequently cite the lack of formal legal frameworks when declining data requests, even in cases involving serious criminal offenses such as intimate image abuse or credible threats of violence. Meta declines 25% of Pakistani requests citing MLAT absence, while X uses this justification to refuse virtually all cooperation[49].

This creates a system where criminal accountability depends not on the severity of harm or clarity of domestic law, but on global community guidelines of social media platforms that are not contextualised to the lived experiences of Pakistani women, resulting in widespread impunity for heinous incidents of TFGBV.

7.3.2 The Structural Form of TFGBV

BEYOND INDIVIDUAL CRIMES
Platform design features systematically enable TFGBV through:
- Engagement-driven algorithms
- Economic incentives for controversy
- Algorithmic amplification of harassment

The enforcement crisis extends beyond individual refusal to share data. It encompasses how platform design features systematically enable TFGBV. This structural dimension helps explain why even successful prosecutions do not result in meaningful deterrence.

Algorithms Boost Harassment

Beyond individual criminal acts, social media platforms enable structural forms of TFGBV through design features which prioritize engagement over safety[50]. Algorithms amplify controversial content that generates high user interaction, creating economic incentives where harassment campaigns receive algorithmic boost precisely because they generate strong emotional responses, targeted campaigns, and sustained user engagement. This creates a chilling effect that forces women's self-censorship online and heightens their vulnerability to harassment[51].

[49]https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Strengthening%20democracy%20by%20reducing%20threats%20to%20women%20in%20politics%20%E2%80%93%20Local%20evidence%20shared%20Solutions.pdf
[50]https://www.gov.uk/government/publications/statement-of-strategic-priorities-for-online-safety/statement-of-strategic-priorities-for-online-safety
[51]https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743341/IPOL_STU(2023)743341_EN.pdf

THE DISPARITY
Women face 27x more online abuse than men on social media platforms
This reflects: Engagement-driven algorithms boosting gender-based attacks
Result: Digital environment actively discourages women's participation

Research indicates that women face 27 times more online abuse on social media platforms than men[52]. The disparity reflects not random hostility but patterns where platforms' engagement-driven algorithms boost gender-based attacks as they generate strong emotional responses and sustained user interaction. The result is a digital environment where women's socio-economic and political participation is actively discouraged through repeated exposure to hostility.

7.4 Regulatory Inadequacy and International Models

PAKISTAN'S CURRENT APPROACH
SMRA's 24-hour content removal = Treats symptoms, not causes
Focus: Reactive post incident
Missing: Prevention of harassment patterns + structural fixes

Given the platform non-cooperation challenges documented above, Pakistan's regulatory response proves equally inadequate in addressing platforms' central role in enabling TFGBV. The 2025 PECA amendments have introduced the SMRA with expanded platform oversight powers, but the framework focuses primarily on content takedown rather than addressing the structural features that enable sustained harassment campaigns[53].

The SMRA's 24-hour content removal mandate targets symptoms rather than causes. While rapid post deletion provides immediate relief for TFGBV victims, it stops short of preventing the patterns of abuse that create hostile digital environments for women. More critically, content removal without criminal prosecution enables perpetrators to continue their acts with minimal consequences, perpetuating the impunity crisis identified throughout this analysis.

7.5 International Best Practices

INTERNATIONAL MODELS
Australia's eSafety Commission: Addresses content + underlying platform behaviours

Pakistan's approach: Reactive content removal only
UK's Ofcom: Requires platforms to address design features, algorithms, revenue models

By comparison, international examples illustrate more comprehensive approaches to platform accountability. Australia's eSafety Commission addresses both content moderation and the underlying platform behaviours that enable online harm[54]. Similarly, the UK's Ofcom operates under legislation requiring platforms to address design features, algorithmic amplification, and revenue models that enable technology-facilitated violence against women and girls[55].

The way international regulatory frameworks effectively function confirms that addressing structural TFGBV requires comprehensive responses targeting the business models and design features that enable abuse. This approach contrasts sharply with Pakistan's reactive content removal focus, which leaves underlying violence-facilitating systems intact while enabling perpetrator impunity through limited platform accountability.

7.6 The Enforcement Paradox and Cycle of Impunity

THE PARADOX
Pakistan develops specialized cybercrime investigation capacity
But remains dependent on international private entities that:
- Operate beyond jurisdiction
- Refuse data sharing cooperation
- Control access to evidence needed for prosecution

The current system creates an enforcement paradox where Pakistan's criminal justice institutions develop specialized capacity to investigate technology-facilitated crimes while remaining dependent on international private entities that operate beyond their jurisdiction and refuse data sharing cooperation. This dependency means that even perfect domestic legal frameworks and unlimited investigation resources cannot guarantee justice for TFGBV survivors when platforms control access to the evidence needed for prosecution.

[52]https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech
[53]https://www.na.gov.pk/uploads/documents/679255ee36f45_595.pdf
[54]https://www.esafety.gov.au/sites/default/files/2024-10/ACMA-eSafety-annual-report-2023-24.pdf
[55]https://www.gov.uk/government/publications/statement-of-strategic-priorities-for-online-safety/statement-of-strategic-priorities-for-online-safe

THE VICIOUS CYCLE
Platform non-cooperation → No deterrent effect → Perpetrators choose "safe" platforms
→ Survivors lose faith → Society gets message that TFGBV has no consequences
→ More perpetrators emboldened → Cycle continues

The non-cooperation in data sharing, conflicts between global community guidelines, domestic criminal law, and features on structural platforms that amplify harassment collectively perpetuate a cycle where inadequate institutional responses enable continued abuse. When platforms provide safe havens for anonymous perpetrators through non-cooperation with law enforcement, the deterrent effect of criminal law disappears entirely. Over time, perpetrators strategically choose platforms that offer impunity, survivors lose faith in justice systems, and the broader message sent to Pakistani society is that TFGBV carries minimal consequences, regardless of legal prohibitions.

The enforcement crisis represents more than a technical challenge; it constitutes a fundamental breakdown in the rule of law for TFGBV cases. Until Pakistan develops regulatory frameworks that compel meaningful platform cooperation and address platforms' structural role in enabling TFGBV, these issues will continue undermining women's digital safety and civic participation in Pakistan's increasingly digital society.

RECOMMENDATIONS

Addressing Pakistan's TFGBV crisis requires comprehensive interventions spanning legal reform, institutional capacity building, technological accountability, and social transformation. These recommendations target four critical dimensions:

- **Legal Reform and Institutional Capacity Building** - Strengthening domestic legal frameworks and enforcement mechanisms, including dedicated TFGBV legislation and enhanced resources for LEAs
- **Platform Accountability and Cooperation** - Ensuring technological companies provide data and coordinate with authorities through robust regulatory frameworks
- **Prevention and Social Transformation** - Challenging underlying social attitudes through awareness campaigns and education initiatives
- ***Coordination and International Advocacy*** - Establishing mechanisms for sustained, coordinated responses at international and regional levels

8.1 Legal and Institutional Reforms

8.1.1 Create Dedicated TFGBV Legislation within PECA

LEGISLATIVE PRIORITY
Insert dedicated TFGBV chapter in PECA with:
- Clear definitions of deepfakes, image-based abuse, doxxing
- Distinct cognizable vs non-cognizable categories by severity
- Aggravating factors for enhanced penalties

A dedicated TFGBV chapter must be inserted into PECA with clear definitions of emerging forms including deepfakes, image-based sexual abuse, doxxing, and coordinated harassment campaigns. This specialized legislation should establish distinct categories for cognizable and non-cognizable offenses based on severity, specify aggravating factors for enhanced penalties.

8.1.2 Expand Cyber Crime Police Stations and Investigation Capacity

GEOGRAPHIC EXPANSION
Target: Minimum 1 cybercrime police station per district
Priority: Underserved provinces
Staffing: Maximum 200 complaints per investigation officer annually

The NCCIA must establish additional cybercrime police stations to ensure accessible justice for TFGBV survivors across Pakistan's diverse geographic landscape. A minimum of one cybercrime police station per district should be established, with priority given to underserved provinces. Each station must maintain adequate staffing levels with a target ratio of no more than 200 complaints per investigation officer annually to ensure quality investigations and opportunities for specialization.

8.1.3 Establish Specialised TFGBV Investigation Units with Adequate Resources

SPECIALIZED UNITS
- Minimum 20% female officer composition
- Trauma-informed interviewing training
- Dedicated budget allocation per TFGBV case
- Digital forensics capability
- Victim support protocols

Dedicated TFGBV investigation units must be established within each cybercrime police station with minimum 20% female officer composition, specifically trained in trauma-informed interviewing. Additionally, each TFGBV case should receive a dedicated budget allocation to enable proper investigation procedures, digital forensics, and victim support.

8.1.4 Implement Survivor-Centric Evidence Handling Protocols

EVIDENCE PROTECTION PROTOCOLS
- Secure storage with limited access controls
- Mandatory consent procedures for evidence viewing
- Trauma-informed collection techniques
- Time-sensitive preservation for ephemeral content
- Disability inclusivity

Comprehensive protocols for handling TFGBV cases must prioritise survivor dignity, ensure secure storage of evidence with limited access controls and establish mandatory consent procedures for evidence viewing. Officers must be trained in trauma-informed evidence collection and interviewing techniques and time-sensitive preservation procedures for ephemeral digital content. These protocols must also accommodate the specific needs of survivors with disabilities, including accessible communication methods and reasonable accommodations during the interviewing and evidence collection process.

8.1.5 Create Unified Digital Complaint and Case Management System

INTEGRATED SUPPORT SYSTEM
- 24/7 TFGBV helpline with trained female counsellors
- Integration with existing helplines (MHR, NCSW, Virtual Women Police Station)
- Integration with other GBV services including legal aid, shelter homes etc.
- Multi-language digital complaint portal
- Digital identity verification

A dedicated 24/7 TFGBV helpline, located within NCCIA with trained female counsellors, must provide immediate support and crisis intervention to survivors of TFGBV. This helpline must be integrated with existing helplines across Pakistan, including those operated by the Ministry of Human Rights, National Commission on the Status of Women, Virtual Women Police Station of Punjab Police, and other provincial police department helplines to ensure coordinated response and referral mechanisms. The system must leverage and incorporate the advanced technological infrastructure developed by Punjab Safe Cities Authority, learning from their leading practices in digital reporting and verification systems. A comprehensive digital complaint portal with digital identity verification mechanisms must also be established with multi-language support to eliminate in-person verification requirements. Additionally, consolidated feedback mechanisms must be integrated to continuously monitor system effectiveness and survivor satisfaction.

8.2 Platform Accountability and Regulatory Framework

8.2.1 Mandate Emergency Platform Cooperation and Reporting Mechanisms

EMERGENCY PROTOCOLS
- 4-hour BSI sharing for high-risk TFGBV cases
- Platform-specific TFGBV reporting in local languages
- Real-time case tracking systems
- Transparent appeals processes

Emergency 24-hour BSI sharing protocols with Social Media Platforms must be mandated for high-risk TFGBV cases involving intimate image abuse, deepfakes, or credible threats of offline violence. Additionally, regulatory requirements should mandate that platforms develop platform-specific TFGBV reporting categories in local languages, with real-time case tracking systems, and transparent appeals processes.

8.2.2 Establish TFGBV Complaint Mechanisms within Regulatory Framework

SMRA TFGBV PROTOCOLS
- Step-by-step complaint procedures
- Mandatory timelines for response
- Inter-agency coordination protocols
- Emergency response for high-risk cases

The SMRA must develop detailed step-by-step procedures for TFGBV complaint receipt, investigation, and resolution, including mandatory timelines and clear inter-agency coordination protocols. Emergency response protocols for high-risk TFGBV cases must also define immediate content removal procedures.

8.3 Prevention and Social Transformation

8.3.1 Address Toxic Masculinity and Root Causes Through Comprehensive Awareness Programs

TARGETING ROOT CAUSES
The disproportionate targeting of women requires interventions
addressing patriarchal attitudes and toxic masculinity driving TFGBV perpetration

The disproportionate targeting of women requires systematic interventions addressing the patriarchal attitudes and toxic masculinity that drive TFGBV perpetration. Targeted awareness campaigns for young men and boys must focus on challenging harmful gender stereotypes, promoting respectful online behaviour and teaching bystander intervention strategies to interrupt harassment.

8.3.2 National Digital Citizenship and Education Programs

EDUCATION STRATEGY
- Digital citizenship curricula for educational institutions
- Community-based programs with religious leaders
- Media literacy programs (deepfake detection, algorithmic bias)
- Workplace digital safety trainings
- Survivor-led awareness initiatives

National digital citizenship curricula for educational institutions should be designed and implemented to address healthy online relationships, digital consent, consequences of TFGBV, and positive masculinity models. Community-based education programs must work with religious leaders, community elders, and traditional authority figures to promote women's digital rights within culturally sensitive frameworks that resonate with local communities.

Comprehensive media literacy programs should teach recognition of manipulation tactics, identification of TFGBV patterns, deepfake detection, and understanding of algorithmic bias that amplifies harassment. Workplace digital safety training for both public and private sectors must include specific modules on preventing workplace-related TFGBV and creating respectful online work environments. Survivor-led awareness initiatives should be organised to amplify women's voices, and peer education networks should train young women and men as digital safety advocates in their communities.

8.4 Coordination and International Advocacy

8.4.1 Establish National Coordination and Advocacy Mechanisms

NATIONAL COORDINATION STRUCTURE
- National TFGBV Task Force (multi-stakeholder)
- Annual TFGBV assessment reports
- Parliamentary advocacy networks
- Inter-provincial coordination mechanisms

A National TFGBV Task Force comprising government agencies, civil society, academia, and private sector representatives must coordinate policy development and ensure sustained political attention across all levels of government. Annual TFGBV assessment reports should evaluate policy effectiveness and guide evidence-based improvements in institutional responses. Parliamentary advocacy networks must maintain legislative support while inter-provincial coordination mechanisms ensure protection regardless of geographic location within Pakistan.

INTERNATIONAL STRATEGY

- Regional coalitions (South Asian + Muslim-majority countries)
- UN engagement for platform accountability
- Technical assistance partnerships

Regional advocacy coalitions with South Asian and Muslim-majority countries must leverage collective power to influence international regulations and ensure platform accountability from a Global South perspective. Concurrently, international legal cooperation frameworks, UN engagement strategies for platform accountability, and technical assistance partnerships with advanced regulatory jurisdictions should be established to advance comprehensive TFGBV regulatory standards that reflect diverse cultural contexts and legal systems.

ACRONYMS

List of Acronyms

AI	**Artificial Intelligence**
BSI	**Basic Subscriber Information**
CEDAW	**Convention on the Elimination of All Forms of Discrimination Against Women**
DRF	**Digital Rights Foundation**
FIA	**Federal Investigation Agency**
GBV	**Gender-Based Violence**
ICT	**Information and Communication Technology**
MoHR	**Ministry of Human Rights**
NCCIA	**National Cyber Crime Investigation Agency**
PECA	**Prevention of Electronic Crimes Act**
PTA	**Pakistan Telecommunication Authority**
SDG	**Sustainable Development Goals**
SMRA	**Social Media Protection and Regulatory Authority**
SMPs	**Social Media Platforms**
TFGBV	**Technology-Facilitated Gender-Based Violence**
UNFPA	**United Nations Population Fund**
UN SDG 5	**United Nations Sustainable Development Goal 5 (Gender Equality)**
UN SDG 16	**United Nations Sustainable Development Goal 16 (Peace, Justice, and Strong Institutions)**

UK International Development
Partnership | Progress | Prosperity

Awaz اواز

LAS
LEGAL AID SOCIETY

UNFPA
The United Nations sexual and reproductive health agency