



TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TFGBV) IN LESOTHO

LEGAL FRAMEWORK AND PROSECUTION BRIEF

LEGAL POSITION: Lesotho already criminalises some technology-facilitated abuse, especially under the Counter Domestic Violence Act, 2022. The difficulty is that the law is fragmented and the clearest TFGBV offence is limited to people in a domestic relationship. Other statutes can prosecute particular conduct such as threats, extortion, abusive calls, unlawful disclosure of personal information or sexual coercion, but they do not yet create one complete TFGBV offence framework.

What TFGBV means in legal terms

TFGBV is gender-based harm committed, enabled, repeated or amplified through phones, messaging applications, social media, email, online platforms or other digital technologies. Legally, the important question is not only that technology was used, but whether the conduct fits an existing offence or statutory protection: technological abuse, stalking, threats, extortion, sexual coercion, unlawful publication, misuse of personal information, workplace harassment or child sexual exploitation.

Key statutes and provisions

LAW	KEY PROVISIONS	WHAT THE LAW SAYS IN SIMPLE GBV/TFGBV TERMS	WHAT THIS MEANS FOR PROSECUTION
Counter Domestic Violence Act, 2022	s.2; s.3; ss.4–13; s.28(1)(e); s.28(2)(f); s.29	The Act directly recognises technological abuse and electronic stalking as forms of domestic violence. This includes repeatedly sending abusive or offensive electronic messages, and using technology to send, share, expose or display violent, nude, semi-nude, sexual or sexually suggestive material. It also allows survivors to seek protection orders and places duties on police and prosecutors.	This is the strongest direct law for TFGBV where the victim and perpetrator are in a domestic relationship. Police can investigate and charge technological abuse or electronic stalking, while also helping the survivor get immediate protection.
Communications Act, 2012	s.44(1)(a); s.44(2); s.45	The Act makes it an offence to use telephone or communication services to send abusive, threatening or obscene communications. In GBV cases, this can include threatening calls, repeated abusive phone contact, sexual threats or obscene messages sent through communication services.	This can help prosecute some TFGBV cases even where the perpetrator is not a partner or family member, especially where the abuse happens through telephone or communication services.

Penal Code Act, 2012	s.34; s.69; ss.101–104	The Penal Code criminalises threats, extortion or blackmail, and some forms of unlawful publication. In TFGBV cases, this can cover threats to kill or harm someone, threats to release sexual or private material unless the victim gives money, sex or another benefit, and some harmful publications about a person.	Police can use these offences when the digital abuse contains a clear threat, blackmail, sextortion or another recognised criminal act. The fact that the conduct happened online does not stop the normal criminal offence from applying.
Data Protection Act, 2012	ss.2–4; s.29; s.34; s.55	The Act protects personal and sensitive information, including information about a person’s sexual life. It regulates the collection, use, sharing and disclosure of personal information. In TFGBV cases, this can include exposing someone’s private details, sexual information, address, phone number or confidential survivor information without lawful authority.	It can support action in cases involving doxxing, leaking private information, exposing sexual information or misuse of survivor data. Its usefulness may be more limited in some purely personal or household situations.
Sexual Offences Act, 2003	s.2; s.3; s.32	The Act recognises sexual offences committed through threats, extortion, psychological pressure, humiliation or mental harassment. This means technology can form part of a sexual offence where a person is pressured or blackmailed into sexual activity through messages, images or online threats.	This is especially important for sextortion, online sexual coercion and threats linked to sexual acts. The technology is the method used to commit or support the sexual offence.
Children’s Protection and Welfare Act, 2011	s.3; s.22(g), (h), (m); s.24	The Act protects children from abuse, harmful information, sexual exploitation and pornography. In TFGBV cases, this can include online sexual exploitation, grooming-related abuse, circulation of sexual material involving children and exposing children to harmful sexual content.	It provides an important child-protection route, while criminal charges may also be brought under the Sexual Offences Act, Penal Code or other applicable criminal law.
Labour Act, 2024	definitions; s.7(1)–(4); s.206	The Act prohibits workplace violence and harassment, including gender-based violence, sexual harassment, threats, intimidation, bullying and stalking. This can include harassment through WhatsApp, email, social media or other digital platforms where the conduct is linked to work.	It can be used to deal with workplace TFGBV, including disciplinary and labour remedies. If the conduct also amounts to a criminal offence, police can still use the relevant criminal law.

USING THE EXISTING LAW THROUGH A CGPU TFGBV GUIDELINES FRAMEWORK

Purpose of the guidelines framework

The programme objective is to help the Child and Gender Protection Unit (CGPU) turn the existing statutes into a practical police response. The guidelines should help an officer identify the law that applies, collect evidence that proves that offence, protect the complainant and prepare a file that can move to prosecution. They should not create new offences; they should make existing offences usable.

POLICE AND PROSECUTION GUIDELINE FOR TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TFGBV)

— KEY INVESTIGATION AND PROSECUTION PRINCIPLES —

These principles help ensure that TFGBV complaints are handled lawfully, thoroughly and fairly, so that victims are protected, evidence is strong, and perpetrators are held accountable to the law.

1

OFFENCE MAPPING AT FIRST REPORT



Record the conduct first, then match it to the law. Where there is a domestic relationship, consider technological abuse or electronic stalking under the Counter Domestic Violence Act.

Outside that relationship, test the facts against threats, extortion, abuse, communications, sexual coercion, unlawful publication, misuse of personal information, workplace harassment or child sexual exploitation. A complaint should not be rejected only because there is no single offence called "TFGBV."

2

SIMPLE LEGAL-ELEMENTS CHECKLISTS



For each offence, the guideline should show what must be proved. Examples include the domestic relationship, repetition of electronic stalking, what was sent or shared, the threat made, the advantage demanded, or the coercive sexual circumstances.

This allows investigators to collect evidence that actually matches the charge.

3

STANDARD DIGITAL-EVIDENCE RULES



The guideline should require preservation of the original message, proper time stamp where possible; screenshots showing account name, number, date and time; URLs or profile links; phone numbers and usernames; relevant chats or emails; device information; witness statements; and a clear chain of custody.

The aim is to make digital evidence understandable and usable in court.

4

LAWFUL IDENTIFICATION OF PERPETRATORS



Where an account or number must be linked to a person, the guideline should state the lawful route for obtaining subscriber, device, network or platform information.

It should distinguish what CGPU can request directly, what requires legal authority such as a court order, and what should be escalated to specialised investigators or prosecutors.

5

PROTECTION AND PROSECUTION TOGETHER



For cases under the Counter Domestic Violence Act, the guideline should link criminal investigation with available protection orders.

Officers should assess urgent risk, connect complainant to referral for further circulation of material and assist the complainant to access protective remedies while the criminal case proceeds.

6

EARLY PROSECUTOR CONSULTATION AND LEGAL GAPS



Difficult TFGBV files may involve several statutes or unfamiliar digital evidence. The guideline should provide for early prosecutor consultation where the charge is uncertain or evidence needs specialised treatment.

Where harmful conduct does not fit any existing offence, CGPU should still record the complaint, preserve evidence, use any available protection, and classify the matter as a legal gap for future reform.

Bottom line: the strongest immediate contribution of this programme is a practical CGPU guideline that tells an officer what law may apply, what must be proved, what evidence must be collected, what protection is available, and when prosecutor or specialised assistance is required.