acaps

Gender-Based Violence AoR
Global Protection Cluster

UNFPA

TECHNOLOGY - FACILITATED

GENDER-BASED VIOLENCE IN NORTHWEST SYRIA

Table of contents

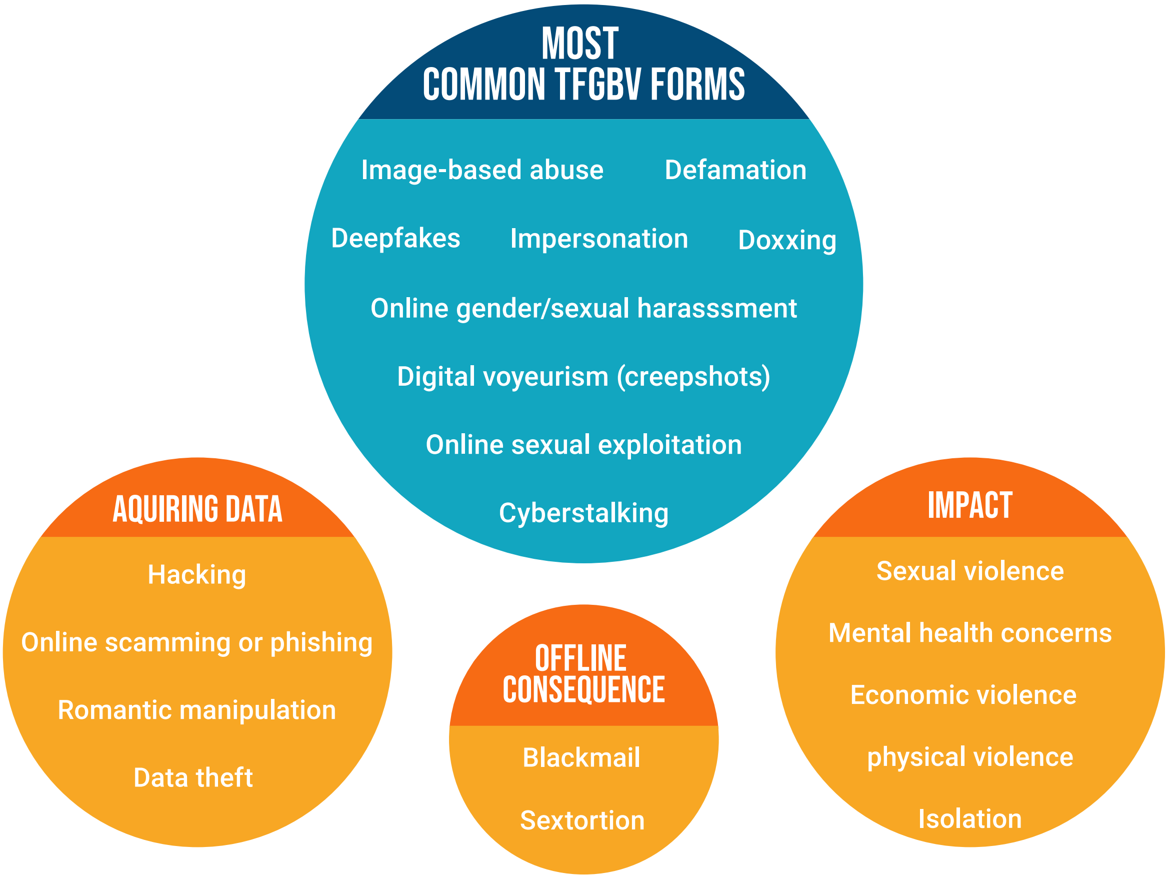
List of Acronymns

ACRONYM	FULL TERM
TFGBV	Technology-Facilitated Gender-Based Violence
GBV	Gender-Based Violence
NWS	Northwest Syria
IDP	Internally Displaced Person
FGD	Focus Group Discussion
KII	Key Informant Interview
HTS	Hay’at Tahrir al-Sham
UNFPA	United Nations Population Fund
GIWPS	Georgetown Institute for Women, Peace and Security
IBA	Image-Based Abuse
AI	Artificial Intelligence
MHPSS	Mental Health and Psychosocial Support
AoR	Area of Responsibility
E&E	Equity and Empowerment (organization referenced in the report)
BBC	British Broadcasting Corporation
AJ	Al Jazeera
IBM	International Business Machines Corporation
SJAC	Syria Justice and Accountability Centre

Overview

Technology-facilitated gender-based violence (TFGBV) is a widespread and rapidly growing concern across Northwest Syria (NWS). TFGBV is driven by limited digital literacy, the accumulated effects of protracted conflict, and entrenched conservative gender norms, resulting in the weaponisation of the Internet and significant shame and victim blaming. TFGBV is further aggravated by a lack of legal frameworks governing cyber violence and ineffective law enforcement, resulting in perpetrators operating in a climate of near-total impunity, leading to a lack of accountability. Multiple forms of TFGBV are often reported in NWS simultaneously, maximising harm to targeted groups or individuals and leading to severe real-life consequences, including financial and sexual exploitation, mental health challenges, social exclusion, and restricted access to livelihoods, education, and other essential services. Conservative cultural norms, a lack of effective authorities, and low digital literacy led to the pervasive underreporting of this issue, as there is fear of social stigma and the risk of further violence from survivors' immediate family and broader community, including so-called 'honour killings'. TFGBV's impact has been further aggravated by the accumulated effect of humanitarian and socioeconomic circumstances, such as forced displacement, armed conflict, overcrowded IDP camps, the COVID-19 pandemic, the cholera outbreak, and a destructive earthquake in February 2023, driving increasing levels of vulnerabilities of the affected communities and access challenges. TFGBV can affect a wide range of individuals, cutting across gender, age, profession, and vulnerability status. Women and girls – particularly young, unmarried, or digitally active individuals – are most exposed to TFGBV.

Figure 1: TFGBV in Northwest Syria



Source: ACAPS with Data from UNFPA 13/01/2025; IBM accessed 05/04/2025; UNFPA 01/12/2021

Aim of the report

This report aims to inform humanitarian responders and gender-based violence (GBV) service providers in NWS, as well as the broader regional response, of the scale, trends, and impact of TFGBV. The report outlines different forms of TFGBV reported across the region, patterns and trends, perpetrator and survivor profiles, the main tools and platforms perpetrators use, and online and offline impacts related to the phenomenon. The report also provides an analysis of the interconnections between TFGBV and the humanitarian response, and information on access, availability, and the main gaps related to specialised survivor services. This analysis aims to inform strategic planning, GBV programming, and GBV risk analysis and contribute to incorporating TFGBV risks in protection and gender analysis frameworks and advocacy.

Methodology

This report is based on primary data collection, including 15 interviews with GBV and TFGBV experts, journalists, activists, and NGO workers; seven focus group discussions with women and girls from affected communities, GBV service providers, and online activists; and analysis of case studies provided by key experts. Purposive sampling has been applied to ensure a high level of expertise, gender and age diversity, and appropriate geographical coverage. Primary data collection was designed to ensure the safety and confidentiality of the respondents and effective data protection protocols. Primary data was complemented by a secondary data review of English and Arabic humanitarian reports and media sources.

This report refers to Northwest Syria (NWS), which is here defined as the northern parts of Idleb governorate and northern and western parts of Aleppo governorate. Primary data was collected between November 2024 and March 2025 both remotely and in person in Azaz (Aleppo governorate) and Idleb city (Idleb governorate).

Limitations

This report is based on qualitative data analysis. Information on the prevalence and impact of TFGBV in NWS remains scarce and anecdotal, making it impossible to draw representative findings. Discussing TFGBV and other forms of GBV is perceived as sensitive, limiting the amount of publicly available information. TFGBV is a new and under-researched area of focus in the GBV sector, with multiple terms and definitions being used interchangeably, presenting a challenge to correctly coding TFGBV forms and occurrences.

© UNFPA Sudan

Key messages

- GBV underreporting has been a persistent challenge in the Syria response. TFGBV reporting levels in NWS, by extension, are also extremely low, driven by intense social stigma, fear of further violence or retaliation, lack of trust in ineffective legal systems, and very limited availability of specialised services. Survivors, particularly young women and girls, face victim blaming and community backlash, with cultural norms amplifying shame and deterring disclosure, even when specialised GBV services are available.
- Adolescent girls, young female IDPs, widows, and women heads of households are among the groups most exposed to TFGBV risks. This vulnerability stems from patriarchal gender norms aggravated by low digital literacy, economic precarity, and reliance on online platforms for social interactions, education, income, and access to services. Intersectional factors that make women and girls in Syria even more acutely at risk of TFGBV include disability, financial vulnerability, public professions, and sexual orientation and gender identity characteristics. Journalists and female activists and leaders face significant risks as a result of their considerable online presence.
- The primary motivations behind TFGBV in NWS include financial and sexual exploitation, revenge or coercion, defamation or causing reputational harm, or simply to threaten, cause harm to, or harass the targeted individual.
- TFGBV frequently escalates from digital threats to offline consequences, including physical and sexual violence, so-called 'honour killings', and forced marriage. This continuum of harm, aggravated by the region's conservative and conflict-affected context, isolates survivors from access to education, livelihoods, and public life. The digital nature of this abuse means that images and materials used to perpetrate it often remain accessible for long periods, leading to continuing victimisation.
- Survivors have minimal access to tailored TFGBV services, with legal support nearly non-existent as a result of absent legal frameworks and law enforcement. Psychosocial support and digital safety trainings are scarce and health services rarely address TFGBV-specific trauma, leaving survivors reliant on inadequate informal networks, perpetuating cycles of vulnerability.
- TFGBV incidents spike during times of major political or humanitarian developments, which increase vulnerability and reliance on digital platforms, exposing women and girls to exploitation, scams, and blackmail. The recent conflict and political developments across Syria triggered increased returns and population movements, which are likely to aggravate the prevalence of TFGBV.
- Humanitarian workers are both at risk of TFGBV and, in some cases, perpetrators. Humanitarian crises aggravate the risk of TFGBV and humanitarian operations can further compound it through the abuse of power dynamics embedded within aid delivery, the insecure collection of sensitive data, and the deployment of poorly designed digital aid systems, which can enable data breaches and unwanted surveillance. As technology becomes integral to aid delivery, understanding these interconnections is critical to safeguarding affected populations and responders alike.

© UNFPA Palestine

Contextual characteristics of TFGBV in NWS

TFGBV is a widespread and growing issue across NWS, as confirmed by all experts interviewed for this report (KII 06/12/2024; KII 23/12/2024; KII 21/01/2025). While TFGBV is a global phenomenon, the scale of the problem and severity of its impacts are context specific. In NWS, the scale of TFGBV is aggravated by the region's social, political, and economic instability, with peaks in reported cases often coinciding with major political or humanitarian developments (KII 23/12/2024; KII 21/01/2025; KII 19/12/2024). The convergence of armed conflict, displacement, economic hardship, cultural conservatism, weak governance, and rapid technological adoption without adequate digital literacy or safeguards creates fertile ground for digital abuse. TFGBV is shaped by deeply embedded gender norms and unequal power dynamics that enable control, surveillance, and exploitation based on gender, disproportionally affecting women and girls.

What is technology-facilitated gender-based violence?

Technology-facilitated gender-based violence (TFGBV) is an act of violence that is committed, assisted, aggravated, and amplified in part or fully by the use of information and communication technologies or other digital tools, perpetrated by one or more individuals against a person on the basis of their gender (UNFPA 03/2023; GIWPS 06/2024).

TFGBV manifests in various forms, many of which are evolving as new technologies develop and new ways of perpetrating harm emerge. TFGBV can occur both online and offline, as it can be perpetrated through any type of technology – old and new – such as phones, GPS tracking devices, drones, or recording devices not connected to the Internet. Often, TFGBV creates a continuum of online and offline abuse leading to grooming and GBV, including acts of physical, sexual, psychological, and/or economic violence (UNFPA 03/2023 and 13/01/2025).

TFGBV is a particularly dangerous type of GBV, as it can be anonymous, automated, and perpetrated remotely, publicly, and continuously against a large number of people (UNFPA 13/01/2025 and 03/2023). TFGBV is difficult to track, scarcely regulated, and widely underreported, leading to impunity. It can also be perpetuated, as erasing or removing TFGBV content is often difficult, leading to compounded trauma.

Although TFGBV can affect anyone, it remains inherently gendered and shaped by power imbalances and restrictive social norms, disproportionately affecting women and girls. Women who occupy public positions, in particular, face higher TFGBV risks, including online harassment and threats designed to silence and disempower them.

It is estimated that between 60–70% of women globally have experienced at least one form of TFGBV and 85% have experienced or witnessed online violence. The prevalence is even higher in the Middle East, where 98% of surveyed women had experienced or witnessed online violence against women (The Economist 1/03/2021; UNFPA 13/01/2025 and 03/2023; GIWPS 06/2024).

The main context-specific factors aggravating the scale and impact of TFGBV in NWS are outlined below.

- **Protracted conflict:** the prolonged Syrian conflict has disrupted social structures, deepened poverty, and increased the risk of and exposure to TFGBV, alongside other forms of GBV (Salamatech 15/03/2024).
- **Weaponisation of the Internet and digital spaces:** the Internet has been a key instrument for Syrians since the 2011 revolution and played a dual role as both a tool for activist mobilisation and a weapon of repression, as the authorities and armed groups used the Internet to censor, monitor, and target political opponents (EuroMed Rights 16/06/2021; AJ 20/06/2015).
- **Entrenched gender inequality and conservative gender norms:** women in countries with longstanding or institutionalised gender inequality, such as Syria, tend to experience online violence at higher rates. Patriarchal rules, practices, and understandings of power are among the key causes of TFGBV (Rutgers 2024). In many Syrian communities, women's reputations are closely tied to cultural and religious practices as well as notions of family honour and modesty. As a result, TFGBV survivors face intense social stigma, fear of retaliation from family members (including threats of so-called 'honour-related violence'), and are often blamed for the abuse. This prevents many from seeking help, leading to severe underreporting.

- Fragmented governance: NWS' political environment has been highly fragmented since 2011, with control over different territories divided between the former Syrian government and different opposition and military groups. Following the takeover in December 2024, Hay'at Tahrir al-Sham (HTS), which had already controlled vast parts of NWS, further consolidated control over Aleppo and Damascus, but the situation remains uncertain, with a number of different armed groups controlling different parts of the country, undermining the development and enforcement of legal protections (BBC 13/12/2024).
- **Lack of legal frameworks:** inadequate or conflicting legislation and a lack of law enforcement allows perpetrators to enjoy immunity from punishment, perpetuating the culture of impunity. This is aggravated by women and girls' distrust of the authorities and the nature of TFGBV, which can be committed anonymously and remotely (GBV AoR/Protection Cluster 10/11/2024). The majority of women do not report TFGBV; when they do, they often do not receive adequate follow up and support, as the risks of online violence are either not recognised or perceived as less harmful or dangerous. In many cases, women are simply not aware of channels and procedures to report violence or are accused of 'provoking' violent behaviours (EuroMed Rights 16/06/2021).
- **Economic hardship:** NWS's economy has been adversely affected by the damage and displacement caused by years of conflict, sanctions, the 2023 earthquakes, and rapid currency depreciation, driving up the price of essential goods and services (REACH 30/04/2024). Deteriorating economic conditions create fertile ground for TFGBV, as many perpetrators resort to blackmailing and financially exploiting women and girls to cope with unemployment and financial instability (E&E 03/2022).
- **Low digital literacy:** increasing access to smartphones and the Internet —now essential tools for livelihoods, access to aid, and social interaction – has expanded opportunities for abuse. Unequal access to education and technology means that many people, especially women and girls, have little knowledge of digital security. They are often unaware of how to protect themselves online and rely on second-hand or shared devices and outdated software, making them more exposed to surveillance, hacking, and exploitation. The majority of interview respondents reported a critical lack of knowledge and understanding of TFGBV (KII 20/12/2024 c; KII 15/01/2025; KII 19/12/2024d; KII 19/12/2024).

Forms of TFGBV reported in NWS

There is no close-ended catalogue of TFGBV forms, as they rapidly evolve in line with new technological developments and increasing access to mobile connectivity, social media, and other digital tools. Multiple forms of TFGBV are often inflicted simultaneously to maximise harm against targeted groups or individuals. For example, hacking a social media account or mobile phone can give a perpetrator access to private pictures or videos, leading to threats of disclosing such pictures (image-based abuse), distributing private information (doxxing), and/or economic or sexual exploitation (sextortion), often leading to sexual violence, harassment, defamation, or other real-life forms of GBV, which can potentially escalate to so-called 'honour killings' due to the culture of victim blaming.

The primary motivations behind TFGBV in NWS include financial and sexual exploitation, revenge, coercion, defamation or reputational harm, or simply to threaten, cause harm to, or harass the targeted individual (KII 21/01/2025; FGD 13/03/2025). This shows that TFGBV is almost always intended to cause severe real-life consequences and should not be underestimated as a purely online phenomenon.

Nearly all those interviewed for this report highlighted blackmail as a primary concern and result of most of the TFGBV forms outlined here. Perpetrators often use pictures or videos shared in goodwill or obtained via hacking or coercion to demand money, sexual favours, or coerce survivors into sharing more explicit content under threat of exposure. This can push victims to generate debt or engage in risky income-generating practices, expose them to sexual assault, or lead to physical violence by perpetrators or the survivor's family, causing life-threatening consequences.

> In one case, a girl who sent private photos to a man with whom she was in a relationship was later threatened with online publication of the pictures unless she paid the perpetrator. As she was unable to collect the amount demanded, she resorted to drug trafficking and was eventually arrested and imprisoned (KII 06/12/2024).

TFGBV is used not only to target individuals but also as a tool of exerting broader gendered social control. Some perpetrators aim to humiliate, defame, or damage reputations, particularly in a society such as NWS, where honour and gender norms are deeply intertwined. In some cases, TFGBV is used strategically to force women into silence, deter their participation in public life, or systematically harm specific groups, such as women journalists, activists, or humanitarian workers.

The most pertinent forms of TFGBV in NWS, highlighted by GBV experts, online activists, and affected communities, are outlined below in order of the frequency with which each form was raised as a priority concern.

ACQUIRING DATA	
Hacking	The use of technology to gain illegal or unauthorised access to online systems, accounts, computers, or mobile devices
Online scams or phishing	The use of fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data
Data theft or fraudulent data recovery by phone repair technicians	Retrieving, accessing, and extracting private content from phones during repairs or resale
Romantic manipulation	Feigning trust and romantic relationship to manipulate someone into sharing private photos or videos
MOST COMMON TFGBV FORMS	
Image-based abuse	Using images or videos to coerce, threaten, harass, objectify, or abuse a survivor
Deepfakes	Digital images and audio that are artificially altered or manipulated by AI and/or deep learning
Impersonation	Stealing someone's identity to threaten, intimidate, discredit, or damage a persons reputation
Defamation	Public release and spreading of exaggerated or false information damaging to a person's reputation with the intent of humiliating, threatening, discrediting, humiliating, or punishing the survivor, public figures in particular
Online gender/sexual harassment	Use of technology to repeatedly contact, annoy, threaten, or scare another person through unwelcome, offensive, degrading, or insulting verbal comments and images
Online sexual exploitation	Use of communication technologies, such as cell phones, email, social networking sites, chat rooms or online sites and apps, to commit or procure sexual assault or abuse
Cyberstalking	Use of technology to monitor and stalk someone's activities in real time or by collecting past digital traces
Doxxing	Non-consensual disclosure of personal information, enabling physical targeting or attempts to undermine someone's reputation or credibility
Digital voyeurism (creepshots)	Offline form of TFGBV involving the taking of non-consensual photos or videos of survivors
OFFLINE CONSEQUENCES	
Blackmail	Using pictures or videos shared in goodwill or obtained through hacking or coercion to demand money, sexual favours, or coerce victims into sharing more explicit content under the threat of exposure
Sextortion	Coercing someone into a sexual activity through blackmail, coercion, or threats to release intimate images or sensitive information

- **Hacking** is the use of technology to gain illegal or unauthorised access to online systems, computers, mobile devices, or online accounts to acquire personal information, change or delete information, spread lies to cause reputation damage, or target individuals or organisations (UNFPA 13/01/2025). In NWS, TFGBV perpetrators primarily hack social media accounts and mobile phones to obtain private pictures, videos, or other personal information and use it for the purposes of blackmail or coercion, demanding money or sexual favours/relationships in exchange for not publishing private content. Some perpetrators use this technique to coerce women into marriage, while others impersonate victims on their online accounts to communicate with other men or damage the victim's reputation by publishing incriminating or manipulated content.

> In one case, a man hacked a woman's social media account, stole her private photos, and subsequently blackmailed her, attempting to force her into marriage. The case escalated into an intercommunal conflict between the woman's family and the perpetrator's family, as the man claimed that he received the images directly from her (KII 11/03/2025).

One widely reported method of phone hacking in NWS occurs **via mobile repair shops and the selling of second-hand phones.** Technicians at mobile repair shops, which operate under minimal oversight, access and extract private content — especially images and videos — from (unaware) women's phones. Retrieved or undeleted files, even from factory-reset phones, are then used for blackmail and exploitation. Reports indicate that women's private data is accessed without consent both during repairs and after phones are sold. Some mobile stores sell phones with social media accounts already set up or offer support for women and girls to set up accounts and then retain the passwords, allowing them to access private content (KII 20/03/2025).

> In one case, a young woman who was about to get married gave her phone to a shop for repair. The shopkeeper copied her images and attempted to blackmail her, but was confronted by her fiancé and agreed to delete the photos. While the marriage proceeded, the woman experienced severe stress, as she feared harsh consequences from her family, including potential 'honour violence' (KII 11/03/2025).

A lot of hacking cases include **online scams or phishing,** i.e. perpetrators using fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data, downloading malware, or otherwise exposing themselves to harm (IBM accessed 05/04/2025). In NWS, there are many scams related to supposed job opportunities or humanitarian aid (designed to target women) and English courses or scholarship applications (designed to target girls). These fraudulent links allow perpetrators to hack accounts and devices, install malware, and gain access to data and photos. In some cases, this can escalate to identity theft. In one case, a woman unknowingly clicked a fake aid link and her ID card image was stolen and used to scam others (KII 20/03/2025). Some girls have been targeted by scammers promising to help them recover hacked accounts, but who instead steal more data or demand money, exploiting prior TFGBV and compounding trauma.

- **Image-based abuse (IBA)** means using images to coerce, threaten, harass, objectify, or abuse a survivor, and includes a wide range of behaviours involving taking, sharing, or threatening to share intimate images without consent. These images may be manipulated or sexual in nature, in which case we speak of 'image-based sexual abuse' (UNFPA 01/12/2021). In NWS, most reported TFGBV cases are connected to the unauthorised distribution of personal photos or videos. Many women and girls have had their private images, videos, or messages shared without consent, often by partners or acquaintances, both men and women. Intimate content is shared or published on social media in order to blackmail, shame, or humiliate women and girls, often as revenge after they reject romantic advances. Leaked content often results in severe social stigma, including so-called 'honour killings' or threats of violence, with the targeted woman or girl bearing the burden of shame and perpetrators facing no accountability (KII 15/01/2025; KII 06/12/2024). As one focus group participant noted, ***"If a woman's private pictures are leaked, society will blame her, not the person who spread them"*** (FGD 09/03/2025b).

One particularly prevalent and dangerous form of IBA is sextortion, i.e. coercing someone into a sexual activity through blackmail, coercion, or threats to release intimate images or sensitive information (UNFPA 01/12/2021). Sextortion is highly prevalent in NWS, and often involves stolen or fabricated images and exploiting digital vulnerability and cultural norms to prey on women and girls, leading to escalating violence.

> In one case, a man accessed a woman's photos and blackmailed her with threats of public exposure, leading to the woman being raped. When her family learnt of this, they intended to kill her, so she moved to another area. As a result of the sexual assault, she fell pregnant and had a baby daughter. After some time, she married another man, who would beat her and her two-year-old daughter because of this incident (KII 19/12/2024d).

Another important form of IBA is connected to **AI-generated images or videos, called deepfakes, or other fabricated content.** Deepfakes are digital images and audio artificially altered or manipulated (by AI and/or deep learning) to make someone appear to do or say something they did not actually do or say. Images and videos can be edited to show a person in a compromising position or making controversial statements (UNFPA 01/12/2021). In NWS, AI also presents emerging threats, with manipulated photos and videos used to humiliate or blackmail women and girls in particular. This form of IBA is particularly threatening for women journalists, activists, and humanitarian workers, as they are more recognisable. However, experts also shared cases of ordinary girls having their pictures or videos digitally altered to show revealing, intimate content and being blackmailed by threats of distribution (KII 19/12/2024a; KII 21/01/2025).

> One case that highlights the deeply gendered nature of this type of TFGBV involved a male survivor, whose pictures were stolen and manipulated to depict him as a woman in order to blackmail him, causing severe psychological distress (KII 11/03/2025).

- **Impersonation** is a process of stealing a person's i**dentity in order to** threaten or intimidate them, as well as discredit or damage their reputation (UNFPA 01/12/2021). In NWS, this form of TFGBV is a widespread concern for women and girls, particularly on social media. As one key informant defined, impersonation often occurs when "someone uses your information to create a fake account with your name and starts communicating with people pretending to be you and sharing inappropriate content" (KII 19/12/2024d). Such impostor accounts, which often use stolen or fabricated pictures of women, are used for defamation or extortion. Another dimension of impersonation involves the creation of fake profiles in order to lure victims into conversation and collect personal information. Some perpetrators pretend to be girls to contact other young girls or authority figures and involve them in incriminating conversations, which are documented and later used against them (FGD 09/03/2025a).
- **Defamation** involves the public release and spread of exaggerated or false information that causes reputational damage with the intent to humiliate, threaten, discredit, intimidate, or punish the survivor, public figures in particular (for example, public officials, activists, and journalists) (UNFPA 01/12/2021). In NWS, defamation often occurs on social media, with individuals being accused of inappropriate behaviour. Women, often activists, NGO workers, or other professionals, are deliberately targeted with false narratives to discredit or shame them, leading to severe mental health consequences and loss of employment (KII 06/12/2024). This can occur in systematic, organised campaigns targeting specific women in retaliation for their public activities or to enforce gendered social control, leading to societal rejection or physical harm. There are specific Telegram channels used for mass exposure ('scandalous' channels) (KII 20/03/2025).

> In one public case, a woman doctor in NWS was targeted by a fake account that falsely accused her of engaging in sexual relationships with Turkish officers. The account also posted a picture of this woman without a hijab. The following day, her brother killed her in public, encouraged by bystanders (KII 06/12/2024; SJAC 2/11/2018).

- **Online (gender/sexual) harassment** involves the use of technology to repeatedly contact, annoy, threaten, or scare a person via unwelcome, offensive, degrading, or insulting comments and/or images. This type of harassment is committed by individuals or mobs of male perpetrators, who target people because of their gender, sexuality, or sexual orientation (UNFPA 01/12/2021). In NWS, online harassment is common and deeply gendered, ranging from persistent unwanted messages, explicit pictures, and videos to online sexual harassment and threats of physical or sexual violence in order to coerce the target (predominantly women and girls) into further communication or exploitation. One focus group participant stated: "the most common complaint we receive is about WhatsApp and Facebook messages containing inappropriate pictures or offensive comments" (FGD 13/03/2025). While this tactic is mainly employed to humiliate, it can escalate into real-world stalking, intimidation, or grooming for future sexual assaults. Women active in online spaces, who express their opinions or hold leadership positions, such as activists or students, are often subjected to coordinated harassment campaigns ('mobbing'), hate speech, and bullying designed to silence them. This occurs on social media platforms, particularly WhatsApp and Telegram, both publicly and through direct messages. Some perpetrators create fake accounts to target specific women and girls.

- **Cyberstalking** involves the use of technology to monitor and stalk a person's activities in real-time or by collecting past digital traces (UNFPA 13/01/2025). Stalking and repeated harassment, particularly targeting female students, activists, and journalists, have been reported in NWS, where perpetrators track online activities and location-tagged content to monitor survivors' routines, networks, or movements. This can escalate to real-life stalking, with some perpetrators following their victims by learning their location via social media (FGD 11/03/2025; FGD 10/03/2025).
- **Sexual exploitation through gaming platforms** is now an increasing trend in NWS. Women and girls are being exploited via mobile games and various chat applications. Perpetrators hack online game accounts storing personal photos or videos with the intent to blackmail. There are also cases in which such games offer additional perks or even money to those who upload more pictures or videos. The most concerning manifestation, however, is a new trend called 'coins', in which financial rewards are offered for chatting with people online. The more time a person spends on these applications, the more 'coins' are awarded, which can later be converted into money, leading to addiction or financial dependence on such platforms. Sometimes, the people one chats with offer more money depending on the length and content of the chat, incentivising emotional and sexualised exchanges. This lures women into codependent relationships or effectively provides incentives for them to talk to a large number of men, which one expert described as an "online sex trade". This is a significant concern for adolescent girls, young women, and married women, particularly those with limited access to employment opportunities.

> In one case, a woman was blackmailed through the online game PUBG (a player-versus-player shooter game). A male gamer hacked her phone under the pretence of helping her upgrade her game, accessing her private photos and threatening to leak them unless she provided more intimate images. Her family staged a fake funeral and announced her 'death' to make the blackmailer stop (KII 19/12/2024c; KII A 20/12/2024

- **Doxxing** is a gendered form of online harassment consisting of the non-consensual public disclosure of personal information, for example an individual's home and email addresses, phone numbers, employer and family members' contact information, or photos of their children and the school they attend with the intent of causing physical harm (UNFPA 01/12/2021). Several key informants noted that doxxing also occurs in NWS (KII 06/12/2024; KII 23/12/2024; KII 20/03/2025).
- **Creepshots (digital voyeurism)** is an offline form of TFGBV involving the taking of non-consensual photos or videos, mainly of women and girls, in public places – such as stores, public bathrooms, locker rooms, classrooms, or on the street – as well as in the target's own apartment and spaces considered 'safe' (UNFPA 01/12/2021). Some women in NWS have reported being secretly photographed in public places such as universities or even at home. In one case, a female student was blackmailed by a male peer, who had taken photos of her and her roommates while they slept, later demanding more explicit pictures (KII 20/03/2025).

© UNFPA Türkiye-David Brunetti

TFGBV patterns and trends in NWS

Scale of TFGBV in NWS and patterns and trends over time

The scale of TFGBV in NWS is vast, growing, and often underreported. While the sensitive nature of the abuse and widespread social stigma make precise figures hard to obtain, evidence from service providers and community reports suggests that TFGBV is a widespread phenomenon affecting all genders, but girls and women in particular, across all backgrounds – ordinary civilians, students, activists, and aid workers alike. One key informant indicated that at least 50–60% of women and girls in the region are affected by some form of TFGBV, and these numbers are likely to increase as the population grows and more people return to NWS.

The scale of TFGBV across NWS has been increasing in recent years, driven by increased dependence on digital connectivity, social media, and the Internet for communication, accessing services and humanitarian aid, and income generation. GBV experts reported encountering new TFGBV cases weekly or even daily, highlighting the breadth of the problem (FGD 13/03/2025SCDC 08/10/2024; Protection Cluster 28/03/2023).

TFGBV incidents spike during times of major political instability, humanitarian disruption, and increased social activities. Recent conflict and political developments across Syria have triggered increased returns and population movements, likely aggravating occurrences of TFGBV (KII 20/12/2024 b). Incidents peaked during the COVID-19 lockdowns and February 2023 earthquake, as well as during Ramadan (when aid scams become more prevalent) and periods of heightened political or military activity (KII 20/03/2025; KII 21/01/2025). The COVID-19 pandemic, in particular, aggravated these trends, as more people relied on digital platforms for communication and work, leading to a rise in reported cases of online violence against women (EuroMed Rights 21/05/2021). These surges point to the opportunistic nature of TFGBV, with perpetrators exploiting moments of chaos or vulnerability, when oversight, protection mechanisms, and support are weakest.

As digital accessibility expands, so too does exposure to TFGBV, with more sophisticated technology making it more difficult to detect, track, and regulate (KII 20/12/2024 c; KII 20/12/2024 b; KII 20/12/2024 a). The number of mobile connections in Syria increased by 7% between the beginning of 2024 and beginning of 2025, when nearly 78% of the total population had access to mobile connectivity (compared to more than 82% in Jordan) (DataReportal 03/03/2025 a). At the same time, up to 36% of the population had access to the Internet, 4% higher than at the start of 2024 but significantly lower than in neighbouring Jordan, where access stood at more than 92% at the start of 2025, indicating a high need for digital literacy support as Internet access increases across Syria (DataReportal 03/03/2025 a and 03/03/2025 b). While awareness-raising efforts have led to increased disclosures, underreporting remains a challenge, and the overall trend suggests a worsening situation as technology continues to evolve, significantly increasing TFGBV risks (KII 15/01/2025; KII 19/12/2024 d; KII 19/12/2024).

Patterns and trends across geographic location

There are no clear TFGBV trends across different areas of NWS. Interview respondents underlined, however, that different communities face varied levels of vulnerability to TFGBV and related risk patterns based on location.

- **Urban areas** are more likely to report high numbers of TFGBV cases because there is more access to the Internet and higher levels of digital activity in these areas. Many cases have been reported around universities in urban centres (KII 23/12/2024; KII 20/03/2025).
- **Rural areas** or people originating from rural areas displaced to areas with higher digital access are more vulnerable to TFGBV risks, as they have lower levels of digital literacy and are less equipped to protect themselves online. Respondents named western rural Aleppo as an area where many TFGBV cases have been reported (KII 18/12/2024; KII 20/12/2024 b).
- **Camps hosting IDPs, particularly 'widows camps',** are where many TFGBV cases in NWS have been reported, with most occurring in camps in Idleb (KII 20/12/2024 c). Crowded conditions, lack of privacy and livelihood opportunities, reliance on humanitarian aid, and dependence on mobile phones and social media for aid and income opportunities aggravate IDPs' TFGBV risks, particularly for women and girls (KII 11/03/2025). Camp conditions were created to provide shelter but often result in isolating women and increasing their vulnerability to both physical and digital violence. Camps' remote locations and lack of transportation options further isolate people and reduce access to support services (KII 15/01/2025; SecDev Foundation 03/2024).

- **Digitally networked communities (e.g. neighbourhoods, villages) with dedicated social media (e.g. Telegram) channels** are a particular risk, as any public exposure of private content on such channels would put survivors at higher risk of violence and negative repercussions than when facing similar circumstances in a larger, more anonymous community (KII 21/01/2025).

Types of perpetrators, main tools, and platforms used

There are multiple types of TFGBV perpetrators using various tools, platforms, and tactics to target victims across NWS. While perpetrators are predominantly men explo iting women and girls' emotional and financial vulnerabilities, there are also reports of women perpetrators facilitating access to or gaining incriminating content from other women (E&E 03/2022).

> In one case, a woman secretly entered homes in which other women felt safe and wore lighter clothing, particularly during the summer, and, without their knowledge, took photos of them. She then sent the images to men in another area, who blackmailed the women, demanding money in exchange for not publishing the images. The social consequences were severe, as at least three of these women were divorced by their husbands as a result and divorced women often face stigma and struggle to regain their standing in the community (FGD 09/03/2025 b).

The main types of perpetrators include the following.

- **Individual perpetrators that know the targeted victim,** such as relatives, acquaintances, or community members. This includes ex-fiancés, romantic partners, friends, and family members, who exploit existing trust and access to private data, which women often share with them willingly. These men often initiate their actions through romantic manipulation, creating trust before exploiting (E&E 03/2022). The overlap of emotional betrayal, TFGBV, and social stigma makes this group of perpetrators particularly difficult to address through conventional reporting.

> Many such cases include engaged young women, particularly with fiancés outside Syria. She may have a video call with him without wearing hijab or wearing 'inappropriate' clothes, which the man photographs or records. Then, when the engagement is over, he blackmails her. One key informant cited the case of a woman who was in a relationship and sent the man photos, but later ended up marrying another man. The previous boyfriend blackmailed her, threatening to send the photos to her husband. This led to her arrest by local authorities, on charges of prostitution, for which she spent one year in jail (KII 18/12/2024).

- **Authority figures,** such as teachers, doctors, and humanitarian workers, have been known to abuse their power and use TFGBV tactics for financial or sexual exploitation (KII 17/12/2024; KII 19/12/2024 c).
- **Anonymous individual perpetrators,** often with technical skills surpassing those of their victims, such as hackers, or individuals using fake profiles or AI-generated content. Some operate locally, others from abroad, particularly Europe, collaborating to coerce and exploit women (Direct Syria 21/09/2024). The anonymity of online spaces allows perpetrators to operate with impunity, as it is difficult to trace and hold them accountable (Salamatech 15/03/2024). 74% of self-reported TFGBV survivors in a survey of digital violence in Idleb reported not knowing the identity of their perpetrator (Direct Syria 21/09/2024).
- **Technically enabled community-based perpetrators,** including phone repair technicians, scammers using phishing or posing as representatives of aid organisations, and those recovering deleted data from resold phones. These perpetrators often manipulate women by feigning trustworthiness or offering assistance (SecDev Foundation 03/2024). Many young men and boys in IDP camps have learnt hacking techniques and use these skills to blackmail, which is particularly dangerous in a displacement camp setting, as women are unable to easily relocate, change phones, or access digital support.

- **Organised groups** operating mainly on social media (Telegram, TikTok, and Facebook) and other chat applications, which can target larger groups of women simultaneously, particularly through coordinated phishing scams, data theft, or harassment and blackmail campaigns primarily aimed at defamation and financial extortion. The collective and often automated nature of such attacks allows these groups to operate at scale and target multiple individuals or groups at the same time (UNFPA 03/2023).

  In one case, scammers targeted women searching for missing family members in NWS by pretending to have information on their loved ones. Such scammers often use AI-generated photos to manipulate women into believing their family members are alive and detained, demanding money in exchange for more information or assistance (KII 21/01/2025).

- **State and non-state groups,** including armed groups, who use digital violence against women for political or military purposes (KII 19/12/2024).

Main tools and platforms used for TFGBV in NWS

Facebook, according to all community focus group discussions, is the main platform used to inflict TFGBV in NWS. The most common forms of TFGBV reported on Facebook include defamation, blackmail, online harassment, stealing personal photos, and stalking. Many focus group respondents underlined that Facebook is particularly risky because of its popularity, widespread access, and localised community groups (FGD 09/03/2025 a, FGD 12/03/2025 a, FGD 09/03/2025 b, FGD 12/03/2025 b).

WhatsApp is also widely used by perpetrators, particularly for the purposes of blackmail, direct threats, and sharing unsolicited intimate content and phishing links. Importantly, there are several unauthorised, less secure versions of the app, which are used for data privacy breaches, including Gold WhatsApp and Abu Omar WhatsApp. Many organised groups use specific features – such as the ability to change or mask the phone number, send disappearing messages, or use screenshot-blocking options (initially designed to protect users) – to avoid being traced or reported (KII 21/01/2025; KII 23/12/2024).

Telegram – known for its encrypted chats, private channels, and anonymity-friendly features – has also become a key platform for sharing and monetising exploitative content, anonymous harassment, organised large-scale harassment, and the non-consensual sharing of explicit images. Telegram's loose moderation policies, end-to-end encryption, and ability to host large audiences make it particularly dangerous for facilitating and normalising online sexual exploitation. Adolescent girls are often targeted via direct message or invited into groups under false pretences in the process of grooming for sexual exploitation (FGD 11/03/2025).

One focus group underlined a disturbing phenomenon: mothers actively facilitating the online sexual exploitation of their daughters, some aged 13–14, as a means of generating income. This TFGBV involves the use of mobile phones and messaging platforms such as WhatsApp and Telegram to coerce young girls into engaging in explicit online interactions with men. The mothers, who orchestrate and profit from these activities, earn approximately USD 50/hour, often equipping their daughters with multiple devices to maximise earnings. As one focus group participant noted, ***"girls who become used to this won't be able to escape it later. This will ruin their futures"*** (FGD 09/03/2025 b).

TikTok has become hugely popular among children and adolescents, especially young girls. NGO focus group participants reported that TFGBV perpetrators exploit the platform's algorithm and public commenting system to groom and coerce girls – through validation, flattery, and monetary incentives – into posting increasingly provocative content, such as exploitative livestreams (FGD 11/03/2025).

Instagram is used to hack young women and girls' accounts, gain access to their photos and videos, and manipulate them, all aggravated by the photocentric nature of this tool. TFGBV perpetrators use the app for online grooming, sextortion, and unsolicited contact, alongside harassment campaigns and defamation (FGD 11/03/2025).

Gaming platforms (PUBG, Mariam, Free Fire, and Fortnite) are susceptible to hacking, with perpetrators also exploiting in-game chat or voice features for grooming and manipulation. They build trust, initiate conversations, manipulate into sharing personal contact details or photos, and slowly transition interactions to more private messaging apps, such as WhatsApp or Telegram, where the abuse continues or escalates. Interviewees also noted instances of players' mobile devices being hacked, with perpetrators gaining access to private pictures and videos. (KII 19/12/2024 c).

Chat applications (Yalla Chat, Ya Hala, and Kwai) often offer financial incentives (so-called 'coins') for taking video calls with strangers, putting women and girls at risk of manipulation and online sexual exploitation. These platforms operate at the intersection of economic exploitation, sexual coercion, and digital manipulation. Women with no other means of generating income become particularly dependent on such schemes, making it difficult to disengage and leading to extremely negative mental health effects. One expert reported: ***"We noticed cases of suicide or suicidal thoughts among survivors of these TFGBV cases, and others now have depression and take medication to be able to sleep at night*"** (KII 20/12/2024 a).

Groups most at risk of TFGBV

TFGBV can affect a wide range of individuals across gender, age, profession, and vulnerability status. While patriarchal norms make women and girls – particularly young, unmarried, or digitally active individuals – most exposed to TFGBV, men and boys are also affected, although such cases are less reported. Professionals such as humanitarian workers, journalists, and activists also face heightened risks as a result of the public nature of their roles, while marginalised groups, including displaced people, LGBTQ+ communities, widows, and those with low digital literacy, are especially vulnerable to TFGBV as a result of preexisting exclusion and lack of protection structures (KII 06/12/2024; Rutgers 2024).

Main groups at risk of TFGBV in NWS

- **Adolescent girls and young women are the groups most at risk of TFGBV.** Interview respondents shared that the majority of survivors are girls under the age of 18 (KII 20/12/2024 c). Girls and women who are unmarried, displaced, university students, or generally active on social media and gaming platforms are considered the most at risk (KII 21/01/2025).
- **Women IDPs, particularly widows and women heads of households,** are also highly susceptible to TFGBV as a result of extreme socioeconomic exposure, limited legal protections, and reliance on digital spaces to access aid and livelihoods. These women are often exposed to scams and phishing attacks, with hackers impersonating humanitarian responders (KII 19/12/2024; KII 20/12/2024 c).
- **Women in public roles, such as humanitarian workers, journalists, and social and political activists,** are a TFGBV at-risk group because of their professional exposure and visibility, being targeted for their activism, sharing opinions online, and challenging conservative gender norms (KII 18/12/2024). These groups are particularly at risk of online harassment, coordinated defamation campaigns, and IBA via AI-generated content. As one key informant reported, "threats of rape and other sexual violence are things female GBV staff face, even sometimes from fellow humanitarian workers" (KII 20/12/2024 a).
- **Boys and men are also exposed to TFGBV,** albeit such cases are far less reported. Young boys, particularly those under 18 in displacement camps, face sexual exploitation, blackmail, and harassment on platforms such as Telegram and gaming forums, often resulting in psychological stress, social humiliation, and family conflict. Boys are also targeted by extremist groups for recruitment. Adult men, especially those with financial means or public status, are targeted by organised groups or fake accounts sending sexual content, leading to financial exploitation (FGD 13/03/2025).

A child in NWS was contacted via social media and coerced into joining an extremist group. The recruitment process included persistent online interactions and exposure to extremist content (KII 06/12/2024).

- **Marginalised groups (LGBTQ+, religious minorities, and people with disabilities)** are highly vulnerable to TFGBV as a result of preexisting patterns of discrimination, social exclusion, and limited access to protection services. People with disabilities who rely on online connectivity for the majority of their communication and access to aid and services are more exposed to scams and face severely limited access to protection services (KII 20/12/2024 b). Marginalisation deepens both the risk of targeting and barriers to redress, leaving these groups disproportionately exposed and systematically unprotected.

Impact of TFGBV in NWS

The impact of TFGBV is profound, with significant psychological, social, and economic consequences reported by the survivors (UNFPA 24/01/2024). Such immediate impacts are further aggravated by the region's conservative cultural norms and community surveillance, leading to intense fear of public exposure, as survivors almost certainly face further risk of violence from immediate family and the broader community (KII 06/12/2024). The impact of TFGBV can be felt both online and offline and lead to severe long-term consequences, such as withdrawal from public life and, in extreme cases, death at the hands of family members (KII 17/12/2024).

> A 16-year-old girl was killed by her brother in a so-called 'honour crime' in an IDP camp after WhatsApp messages and images surfaced showing her interacting with a boy (KII 20/03/2025).

Main TFGBV impacts

- **Mental health issues:** survivors experience acute stress and mental health crises, including anxiety and depression, from threats, blackmail, or exposure. Young girls and adolescent survivors are particularly affected, with reports of suicidal ideation and attempts stemming from overwhelming fear (KII 19/12/2024 d).
- **Economic exploitation:** survivors, especially economically vulnerable women and displaced people, are coerced into paying blackmailers or engaging in transactional sex and relationships, pushing them into debt or risky income-generating activities. Some survivors are forced to pay perpetrators multiple times to stop the threats (KII 15/01/2025).
- **Isolation and withdrawal from online spaces:** immediate withdrawal from online and offline spaces is common, with survivors deleting social media accounts and avoiding public activities out of fear. Many survivors stop using mobile phones and social media entirely, isolating themselves from their communities and access to livelihoods, information, and essential services. Self-censorship is widespread, leading to women's reduced representation in public discourse. Female students and activists are notably affected, often halting education or advocacy efforts (KII 11/03/2025; KII 06/12/2024; KII 15/01/2025; FGD 10/03/2025). Some women have started wearing niqab solely to avoid visual exposure and targeting (FGD 12/03/2025 b).
- **Physical violence and retaliation, including so-called 'honour killings':** threats escalate to physical harm, including beatings or 'honour killings' by family members reacting to perceived shame and reputational damage. Some interviewees reported that family-member violence is often more concerning than perpetrator violence (KII 20/12/2024 c).
- **Rape and sexual assault:** online sexual harassment, grooming, and blackmail can escalate into sexual assault, including rape, if a woman is coerced into transactional sex to meet perpetrator demands (KII 19/12/2024 d).
- **Social exclusion and stigma:** survivors endure reputational damage, family rejection, and societal blame, resulting in disownment or forced marriage to mitigate scandal (FGD 13/03/2025; FGD 10/03/2025).

- **Loss of access to education and livelihoods:** TFGBV can cause girls and female students to withdraw from educational activities and women employees, particularly in humanitarian organisations, to lose their jobs. This can be the result of families restricting girls and young women's mobility, employers terminating contracts because of damage to the employee's reputation, and self-withdrawals to avoid shame and further mental distress (FGD 09/03/2025 a; KII 19/12/2024; KII 19/12/2024 d).

> A well-known professional woman in NWS was targeted by an online defamation campaign labelling her an atheist. The resulting public scrutiny led to her resignation, severe depression, multiple suicide attempts, and complete withdrawal from public life (KII 06/12/2024).

- **Forced displacement or restricted mobility:** some survivors must relocate to escape threats or the social consequences of TFGBV (FGD 13/03/2025). Young women and girls often lose their freedom and mobility, as their families prevent them from leaving the house and continuing school, work, or other social engagements (FGD 09/03/2025 a).

TFGBV also has broader effects on communities in NWS, fostering mistrust, reinforcing gender inequalities, and disrupting social cohesion.

- **Normalisation of GBV:** TFGBV reinforces offline patriarchal norms, legitimising hate speech and violence against women. Conservative rural communities are most affected, where traditional gender roles amplify blame on women (KII 06/12/2024).
- **Erosion of trust:** widespread mistrust of digital platforms and institutions is a direct result of TFGBV. Online defamation campaigns create mistrust within communities. Some interviewees reported a weakening of family structures leading to family breakdowns, a lack of trust in communities and traditional support systems, and fractured social cohesion. Defamation campaigns have a particularly negative impact on tight-knit, localised communities in which stigma spreads rapidly (KII 23/12/2024; KII 19/12/2024).
- **Women's reduced participation:** the fear and impact of TFGBV restricts women's access to education, work, and digital spaces, deepening gender inequality. Camp-based and displaced communities see the starkest declines, with families banning phone use or school attendance (KII 11/03/2025; KII 06/12/2024).

© UNFPA Türkiye-David Brunetti

Reporting levels and access to/availability of specialised TFGBV services in NWS

Barriers to reporting and accessing services

TFGBV survivors face significant limitations in reporting incidents and accessing specialised assistance. From a survivor's perspective, fear of stigma, retaliation, and ineffective support systems pose significant barriers to reporting, leaving many without assistance or protection (KII 21/01/2025). The scale of TFGBV reporting in NWS is alarmingly low, with one interviewee suggesting an estimated reporting rate below 5% (KII 11/03/2025).

Fear of social stigma, retaliation (including threats of so-called 'honour killings' or family violence), and victim blaming – all deeply rooted in traditional gender norms and social and cultural dynamics that often fault women for abuse rather than perpetrators – is the single biggest barrier to survivor reporting (KII 21/01/2025). Other barriers stem from a lack of trust in legal and institutional systems (perceived as unresponsive or complicit) and limited awareness of reporting channels (KII 19/12/2024; KII 20/12/2024 a). Women professionals, such as humanitarian workers and activists, may fear job loss or repercussions, further deterring disclosure.

Formal channels such as police or legal systems are rarely used due to inaccessibility and perceived inefficiency. Informal reporting to NGOs or trusted individuals occurs, but even these channels are limited by safety concerns and capacity. (KII 20/03/2025).

Lack of legal frameworks and law enforcement

In NWS, the absence of legal frameworks to address TFGBV is a critical obstacle, as there are no clear laws governing digital violence. Pre-revolution laws from 2011 are outdated, ill-equipped for digital crimes, and unenforced, and the judicial system is ineffective. In some areas, such as Afrin or Azaz, perpetrators have been reported among local authorities and various armed groups competing over different areas, heightening risks for survivors seeking justice. Police responses are limited to basic complaints, as they lack the capacity or will to investigate digital crimes and survivors fear that officials may breach confidentiality or further exploit them. This legal vacuum fosters impunity, discourages reporting, and leaves survivors without formal recourse (FGD 11/03/2025; FGD 10/03/2025; KII 19/12/2024 a).

Available support and main gaps

TFGBV-specialised services are scarce and unevenly distributed across NWS (Salamatech 15/03/2024). The limited GBV services available for TFGBV survivors include mental health and psychosocial support (MHPSS), case management, and awareness-raising initiatives provided by humanitarian NGOs and TFGBV-specialised organisations, such as Equity and Empowerment and Salamatech.

There are also some digital literacy programmes, prevention from exploitation and abuse initiatives, and school-NGO collaborations to create safer online environments (E&E 09/2024). These services are not widely recognised, however, or sufficient in scope and reach, with only a few entities offering specialised TFGBV support.

Quality issues persist as a result of insufficient staff capacity, resource constraints, and a lack of focus on digital safety. Many GBV responders lack TFGBV-specific expertise and caseworkers face security risks limiting their effectiveness. The scarcity of services forces survivors to rely on informal networks (trusted friends or family), though these often lack the capacity or expertise to provide meaningful assistance. As one interview respondent said: ***"we can't trust a lot of people with IT experience because we are not sure they will keep the information safe, and we don't have a lot of trained people with good IT experience to support cases"*** (KII 18/12/2024; KII 19/12/2024 d).

The main gaps in TFGBV services for survivors underlined by focus group respondents include legal, data protection, MHPSS, and health services (FGD 11/03/2025).

Survivors' primary needs include confidential, survivor-centred services, as well as **protection and legal support** in finding pathways to report and achieve accountability.

Digital safety and data protection trainings are necessary with practical tools for managing digital devices and accounts securely and responsibly, mitigating TFGBV risks. More hotlines and online mechanisms for immediate reporting are needed, alongside more community-based education on digital risks.

MHPSS support is too scarce and not tailored to the needs of TFGBV survivors despite their critical need for counselling, as many cases of suicide and suicidal ideation have been reported.

Health services explicitly addressing TFGBV-related physical or psychological harm, such as stress-induced conditions or injuries from family retaliation, are not available.

TFGBV risks and impact for humanitarian operations

TFGBV interacts with the humanitarian aid sector in multiple ways, underscoring the importance of awareness raising, capacity building, and further research to understand the impact TFGBV can have on humanitarian operations, and vice versa. As technology becomes more integral to aid delivery, understanding these interconnections is critical to safeguarding communities and responders alike.

Humanitarian responders can themselves be TFGBV perpetrators, as there are cases of exploitation by humanitarian responders and impostors claiming to be humanitarian responders. In one such case, a medical doctor working for a humanitarian organisation manipulated a young female patient, gained access to her phone and photos, and later attempted to coerce her into marriage, highlighting how positions of power can be abused (KII 17/12/2024; KII 21/01/2025).

Humanitarian responders, particularly women, are also survivors of TFGBV, facing threats including sexual harassment and revenge-driven digital attacks, which can also come from within their own organisations. In one such case, a humanitarian worker let her male colleague borrow her flash drive, which contained sensitive information. Later, the male colleague blackmailed her, threatening to distribute the information (KII 20/03/2025). Power imbalances, professional risks, and fear of reputational harm mean that such attacks often go unreported.

Humanitarian crises aggravate TFGBV risks, with events such as conflict or earthquakes increasing vulnerability and reliance on digital platforms for aid registration and information, exposing women and girls to scams and blackmail. Without robust digital protections, these dynamics undermine trust in aid systems, disrupt service delivery, and put populations at greater risk.

During the earthquake in Syria in 2023, many people lost their phones. In one case, a woman's phone was found and her photos were posted in a local buy-and-sell Facebook group. The post contained her identifiable information and suggested intimate photos were available, asking others to contact for further details (KII 21/01/2025).

Humanitarian operations can also heighten TFGBV risks by collecting sensitive data without adequate safeguards or deploying poorly designed digital aid systems, inadvertently exposing women to cyberattacks and exploitation (KII 19/12/2024).

TFGBV affects humanitarian operations by eroding trust, essential to effective aid delivery, when data breaches or impersonations occur, complicating outreach, service delivery, and support efforts. TFGBV awareness among humanitarian responders remains low; many practitioners prioritise traditional GBV forms, lacking the resources and training to effectively address cyber violence (KII 23/12/2024).

Ways forward: increasing TFGBV service capacity in NWS

TFGBV is still considered a new and emerging form of GBV in Syria and at other global, regional, and local levels of humanitarian coordination (KII 19/12/2024). While certain specialised organisations have expert knowledge of the subject, the response generally lacks the awareness and capacity to manage TFGBV risks. TFGBV experts and activists did share a number of recommendations, which are consolidated below and outline potential steps to mitigate TFGBV risks in the future.

> "We learn case by case, as there is no guidance, no tools, or knowledge about it [TFGBV]" (KII 20/12/2024 c).

Raising humanitarian responder awareness: there is a persistent lack of understanding of what TFGBV entails among humanitarian responders. This needs to be addressed through specialised training and awareness raising for GBV humanitarian responders and service providers at the national, regional, and global levels, as well as among frontline service providers, IT professionals, legal advisors, and community focal points, especially those in hard to reach areas. Awareness raising and education are key to TFGBV prevention and enabling specialised survivor services (UNFPA 11/12/2024).

Raising community awareness: normalising discussions of the different forms of TFGBV and their impacts on women, girls, men, boys, and broader communities is necessary to reduce social stigma and victim blaming, which should help to increase reporting levels (KII 15/01/2025). Digital literacy education should be integrated into school-based and youth programming, targeting adolescent girls and other at risk groups (UNFPA 13/01/2025).

Ensuring the digital safety of humanitarian programmes and operations: policies and digital security safeguards that protect responders and communities alike should be implemented. This could mean the development of comprehensive TFGBV safeguarding policies, data protection policies, and the inclusion of TFGBV in GBV response protocols and codes of conduct. After appropriate mechanisms are established, targeted staff capacity building is also necessary to mitigate the TFGBV risks associated with humanitarian operations. Humanitarian responders should communicate, provide access to aid, and educate only on official websites and verified platforms. Campaigns addressing the risks of phishing attacks using aid-related links or job offers are also necessary to build and rebuild trust within communities targeted by such scams (KII 23/12/2024, KII 21/01/2025). An intersectoral approach and joint TFGBV programming and assessments are recommended, particularly between Child Protection AoR, GBV AoR, and other protection and education actors.

> "The main thing is trust. People need to trust us, and it's difficult after the damage has already happened" (KII 21/01/2025).

Ensuring the digital safety of humanitarian responders: to protect sensitive information, ensure that staff have separate work and personal devices and establish proper processes for data cleaning when devices are returned after a contract ends. Provide data protection training for staff, particularly women aid workers, and ensure clear reporting mechanisms for TFGBV survivors within aid organisations (KII 23/12/2024, KII 21/01/2025; KII 19/12/2024). Humanitarian operations need standardised TFGBV operational guidance, contextualised screening tools, case management protocols, and digital safety templates for frontline responders (UNFPA 11/12/2024).

Advocating for legal frameworks and law enforcement: establishing effective legal frameworks for digital violence and cyber security is necessary to protect people from TFGBV and ensure perpetrators are held accountable. In NWS, collaborative advocacy efforts at the local and national levels will be necessary to raise awareness of the need for regulation, systematic accountability, and the establishment of law enforcement mechanisms. Engaging with local and national authorities in a context-appropriate manner to provide guidance and best practices will be key in the changing political environment (KII 23/12/2024; KII 19/12/2024 a).

Engaging communities in the TFGBV response: successful engagement of communities and community leaders is necessary to address TFGBV risks and raise awareness of community support structures that have the potential to mitigate or aggravate TFGBV risks. There is a need for awareness and capacity building among community leaders on how to respond to TFGBV, lowering the risk of victim blaming and violence escalating to so-called 'honour killings' (KII 21/01/2025).

acaps

Gender-Based Violence AoR
Global Protection Cluster

UNFPA