

Joint stakeholder report: Human rights in the digital context in Lebanon



The Association for Progressive Communications (APC), an organisation in consultative status with ECOSOC, is an international network of civil society organisations founded in 1990, dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communications technologies (ICTs). The APC network has 73 organisational members and 44 associates active in 74 countries, including Lebanon.

Contact address: PO Box 29755, Melville 2109, Johannesburg, South Africa

Website: www.apc.org/en

Contact person: Verónica Ferrari, Global Policy Advocacy Coordinator (veronica@apc.org) (marianne@smex.org)



SMEX is a non-profit that advocates for and advances human rights in digital spaces across West Asia and North Africa. Our vision is for everyone living in West Asia-North Africa and the diaspora to be able to access and engage with the internet, mobile services and other networked spaces safely and without fear of censorship, surveillance or repercussion.

Contact address: Beirut, Lebanon

Website: <https://smex.org/about-us/>

Contact person: Marianne Rahme, Senior Policy Analyst and Alliance Coordinator (marianne@smex.org)

I. Introduction

1. Of the 297 recommendations it received during its previous Universal Periodic Review (UPR),¹ Lebanon supported 179. It did not provide a UPR mid-term report on the implementation of the recommendations. However, a civil society coalition composed of over 30 civil society organisations in Lebanon prepared and submitted a mid-term report in 2024, which includes an assessment of progress on the recommendations Lebanon received and provides its own set of recommendations to support implementation.²
2. This report focuses on human rights online in Lebanon, specifically the situation relating to the recommendations concerning freedom of expression, digital inclusion, gender-based violence and marginalised groups. Another joint report by SMEX and Access Now provides additional information on cooperation with international human rights mechanisms, freedom of expression, data protection and the right to privacy, and attacks and harassment against bloggers, journalists, human rights defenders and political opposition.

II. Context

3. Since Lebanon's previous UPR, significant political shifts have occurred. Joseph Aoun was elected president in January 2025, ending a period of political stagnation. Subsequently, Nawaf Salam formed a new government, which gained parliamentary approval in February 2025.
4. Lebanon is still battling the economic crisis that started in 2019 and the large devaluation of its currency (98% of its value was lost between 2019 and 2024). The impact of the economic crisis was compounded by Israel's war on Lebanon in 2024, which impacted access to the internet and essential goods. Other impacts of the war – particularly on freedom of expression and privacy – also resulted from the documented use of tactics like phishing attacks and the spread of disinformation.³

III. The national human rights framework as it relates to human rights online

5. In Lebanon, while the state constitution protects freedom of expression, online speech has been criminalised⁴ under articles 292, 317, 383-389, 474, 582 and 584 of the Penal Code, which stipulate penalties for defamation, slander and libel, as well

1. Human Rights Council. (2021). *Report of the Working Group on the Universal Periodic Review: Lebanon*. United Nations. A/ HRC/47/5. <https://documents.un.org/doc/undoc/gen/g21/081/45/pdf/g2108145.pdf?OpenElement>

2. Arab NGO Network for Development. (2024). *UPR Lebanon – Mid-Term Report – Civil Society Report*. <https://annd.org/en/publications/details/upr-lebanon-mid-term-report-civil-society-report>

3. SMEX. (2024, 30 September). Digital Rights During the War on Lebanon: September 23-30. <https://smex.org/digital-rights-during-the-war-on-lebanon-september-23-30/>; SMEX. (2024, 3 October). Digital Rights During the War on Lebanon: October 2, 2024. <https://smex.org/digital-rights-during-the-war-on-lebanon-october-2-2024/>; SMEX. (2024, 25 October). Digital Rights During the War on Lebanon: October 24-25, 2024. <https://smex.org/digital-rights-during-the-war-on-lebanon-october-24-25-2024/>; SMEX. (2024, 21 November). Digital Rights During the War on Lebanon: November 21, 2024. <https://smex.org/digital-rights-during-the-war-on-lebanon-november-21-2024/>; SMEX. (2024, 25 September). Digital Rights Amid the War on Lebanon: What You Need to Know. <https://smex.org/digital-rights-amid-the-war-on-lebanon-what-you-need-to-know/>

4. Amnesty International. (2023). *Lebanon: Defamation and insult laws weaponized to silence critics*. <https://www.amnesty.org/en/documents/mde18/7046/2023/en/>

as similar articles of the Publications Law (such as articles 12, 20-23 and 25) and the Military Code of Justice (such as articles 157 and 24). These fail to meet international standards.

6. The proposed New Media Law, set to replace the current Publications Law of 1962 and the Audiovisual Law of 1994, also falls short of international standards and contains numerous concerning provisions that pose a threat to freedom of expression and the press. For example, it upholds criminal penalties for critical speech and even increases prison sentences and fines for insults and defamation.⁵
7. The Right to Access Information Law was adopted by the Lebanese parliament in February 2017, but it has not yet been implemented, and a culture of secrecy continues to dominate the public sector. Article 5 of the Law does not comply with the international standards set out in the United Nations Special Rapporteur Report to the Economic and Social Council in 2000,⁶ as it restricts access to certain information, including information related to national security, foreign affairs and professional and commercial secrets protected by law and information that “undermines the state’s economic interests”.
8. The Lebanese Constitution does not explicitly protect the right to privacy, with only the inviolability of the home protected under article 14. Articles 13 and 8 on freedom of expression and individual liberty have been interpreted to imply privacy protection, but they are insufficient and in practice unenforceable. Law No. 140 of 1999 on the protection of the secrecy of communications stipulates the right to confidentiality of local and international communications, via any means, whether wired or wireless connections. However, another article in the same law undermines the right to privacy by introducing exceptions to it “in case of extreme necessity”. This broad condition was not defined in the law and neither is it governed by specific standards. The documented cases of mass surveillance and use of spyware against journalists and human rights defenders underline the inadequacy of the current legal framework.⁷
9. In 2018, Law No. 81/2018 on Electronic Transactions and Personal Data was passed, but it contains numerous gaps as a result of the concentration of power in the executive branch and inadequate safeguards. These include a lack of a definition of the purposes of data collection and failure to require that data subjects be informed of the collection of their data.⁸
10. The government has adopted a Digital Transformation Strategy (2020-2030) that includes plans to roll out a system of digital public infrastructure to access basic public services and goods. However, as described above, there is currently a lack of legal

5. Ibid.

6. Hussain, A. (2000). *Civil and political rights, including the question of: Freedom of expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 1999/36*. United Nations. <https://docs.un.org/en/E/CN.4/2000/63>

7. Freedom House. (2022). *Freedom on the Net 2022: Lebanon*. <https://freedomhouse.org/country/lebanon/freedom-net/2022>

8. SMEX. (2018, 11 October). An “Ugly” New Data Protection Law in Lebanon. <https://smex.org/an-ugly-new-data-protection-law-in-lebanon/>

and technical measures relating to data protection required to protect human rights in the implementation of the strategy.

11. The legal framework also contains gaps in its protection of the rights of women in digital contexts. The Domestic Violence Law (2014) excludes online spaces, leaving victims and survivors without recourse. There is no legislation that addresses technology-facilitated gender-based violence (TFGBV) and instead, existing laws conflate cybercrimes with TFGBV. For instance, Law No. 81/2018 on Electronic Transactions and Personal Data criminalises “illegal interception” but does not address gendered harassment.⁹

IV. Digital inclusion and connectivity

12. Internet penetration in Lebanon stands at 90.1%.¹⁰ However, this belies the unstable and unreliable nature of internet access, which is categorised by the monopolisation of the telecoms sector and is affected by corruption and poor investment.¹¹
13. Since Lebanon’s last UPR, the economic crisis has continued to impact telecommunications services and users have experienced frequent service disruptions and decreased internet speeds.¹²
14. Israeli strikes on the south of Lebanon during 2024 damaged multiple phone towers, heavily impacting service in that region.¹³ The airstrikes carried out by Israel on southern Lebanon affect internet access and connectivity through their direct impact on infrastructure or indirectly as a result of fuel shortages and increased pressure on generators. Months after the ceasefire, citizens have remained without internet in certain parts of the country and have had to resort to unauthorised internet service providers (ISPs) for internet access.¹⁴ Digital warfare tactics used by the Israeli military included disinformation campaigns and ads on social media.¹⁵ SMEX provided reports and guidance to citizens during this time in the absence of action¹⁶ by the authorities, which failed to address these campaigns, for example, through the provision of reliable and diverse information.
15. Research by the Lebanese Court of Audit (special report No. 2/2022, based on report No. 114/2021) on the country’s telecommunications sector details how public funds have been squandered in the telecommunications sector and it provides recommendations to the government.¹⁷ However, the government has yet to heed the recommendations, resorting instead to price hikes. These measures have negatively impacted quality of service. Furthermore, high tariffs and unreliable coverage have disproportionately impacted the

9. <https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf>

10. Kemp, S. (2024, 23 February). Digital 2024: Lebanon. *DataReportal*. <https://datareportal.com/reports/digital-2024-lebanon>

11. SMEX. (2022). *Billions in Squandered Funds: Court of Audit Report on the Telecom Sector in Lebanon*. <https://smex.org/billions-in-squandered-funds-court-of-audit-report-on-the-telecom-sector-in-lebanon/>

12. Freedom House. (2024). *Freedom on the Net 2024: Lebanon*. <https://freedomhouse.org/country/lebanon/freedom-net/2024>

13. SMEX. (2024, 7 October). Digital Rights During the War on Lebanon: October 4-7, 2024. <https://smex.org/digital-rights-during-the-war-in-lebanon-october-4-7-2024/>

14. Ayyad, S. (2025, 3 June). Telecommunications in South Lebanon: Has the Network Recovered After the Ceasefire? *SMEX*. <https://smex.org/telecommunications-in-south-lebanon-has-the-network-recovered-after-the-ceasefire/>

15. SMEX. (2024, 17 October). Digital Rights During the War on Lebanon: October 17, 2024. <https://smex.org/digital-rights-during-the-war-on-lebanon-october-17-2024/>

16. Ibid.

17. SMEX. (2022). Op. cit.

most marginalised communities in the country including migrant workers, women, gig economy workers and impoverished families.¹⁸

16. The government has resurfaced plans to introduce Starlink services in Lebanon, although previous concerns expressed by the Media and Telecommunications Committee that the introduction of Starlink could evade oversight and result in unlawful access to citizens' data have not been addressed. Other stakeholder concerns, legal and regulatory gaps and the expected very high cost of Starlink services have also yet to be addressed.¹⁹
17. The digital divide has been exacerbated by the COVID-19 pandemic and reliance on the internet for education.²⁰

Recommendations relating to digital inclusion and connectivity

18. Develop a five-year plan to advance the sector, including network upgrades to ensure consistent quality across all of Lebanon. The plan should also focus on enhancing services, particularly digital ones, and prioritise innovation as a strategic pillar to support the growth of small and medium-sized enterprises (SMEs) and start-ups.
19. Update Telecommunications Law No. 431 as part of the development of a robust governance framework for the telecoms sector.
20. Activate the Telecommunications Regulatory Authority and grant it the necessary independence to ensure it can act as an effective and transparent regulator for the benefit of society and users.
21. Advance financial and digital inclusion by setting fixed prices for telecommunications services in line with resident purchasing power.
22. Invest in rural infrastructure, especially power solutions, such as renewable energy and generator back-ups.
23. Ensure gender mainstreaming in the implementation of the Digital Transformation Strategy. Work with all implementing agencies and stakeholders of the strategy towards closing the gender digital divide by recognising the differentiated impact that information and communications technologies (ICTs) have on the lives of women and girls, in all their diversity.
24. Implement transparent and inclusive mechanisms for public consultations with civil society organisations on plans to increase internet access, as mentioned above, and enable the more effective involvement of civil society in the preparation of policies.

V. Freedom of expression online

25. In its third review, Lebanon supported recommendations 150.135 and 150.145 relating to investigation of attacks against journalists, media professionals, bloggers and human rights defenders.²¹ It also noted recommendation 150.133 to ensure that civilians are tried

18. SMEX. (2024). *Searching for Signal: The State of the Telecom Sector in Lebanon (1992-2023)*. <https://smex.org/research-searching-for-signal-lebanons-telecom-project/>

19. Ayyad, S. (2025, 12 June). Starlink in Lebanon: Who does it really serve? SMEX. <https://smex.org/starlink-in-lebanon-who-does-it-really-serve/>

20. Freedom House. (2024). Op. cit.

21. Human Rights Council. (2021). Op. cit.

in civilian courts.²² Yet, as detailed below, journalists, media professionals, bloggers and human rights defenders continued to be harassed, intimidated and tried in criminal courts using criminal insult, slander and libel laws.

26. In the period since Lebanon's third review, SMEX's Muhal Observatory for Freedom of Expression has reported a continuation of summons and arrests of people over their online speech.²³ This has seen the continued use of criminal insult, slander and libel laws to silence dissent, with the main targets being journalists, political figures and LGBTQ+ activists.²⁴
27. Members of parliament and political figures filed the highest number of complaints, with charges ranging from "slander and libel" to "offending the Lebanese president". Public prosecutors have continued to summon residents and ask them to sign a pledge to refrain from making further statements online, without a trial or a judge's decision. Such impositions are illegal, as the authorities do not have the right to force the signing of pre-trial pledges. Such pledges condemn the defendants without a trial being held, thus robbing them of their rights to a fair trial and defence, which are protected and guaranteed by the Universal Declaration of Human Rights.²⁵
28. Between 2017 and 2023, there were more than 800 violations against journalists in Lebanon, including severe beatings by security forces, legal and illegal summons and personal harassment via phones.²⁶
29. Examples of violations in the form of legal actions include that taken against the feminist news platform Sharika Wa Laken. In 2023, its editor-in-chief, Hayat Mirshad, was summoned over the publication of survivor testimonies. The Cybercrime and Intellectual Property Protection Bureau subpoenaed Hayat Mirshad to appear before it, in response to a "libel and slander" complaint filed against her.²⁷ Also in 2023, the Security Bureau summoned the editor-in-chief of The Public Source, Lara Bitar, over an investigation relating to toxic waste.²⁸
30. In 2023, Lebanese TV presenter Dima Sadek was found guilty of slander, defamation and inciting sectarian tensions, in violation of articles 582, 584 and 317 of the Penal Code. This judgment is one of the most severe verdicts issued in Lebanon in a case related to freedom of expression and the first where a sentence of imprisonment was imposed for statements on social media.²⁹
31. Extensive website blocking has continued in the period since Lebanon's third review. In 2020, the Lebanese General Prosecutor ordered the Ministry of Telecommunications to compel all internet service providers to block 28 applications, claiming that these

22. Ibid.

23. <https://muhal.org/en/cases>

24. Amnesty International. (2023). Op. cit.

25. SMEX. (2020, 13 July). Lebanon: New coalition to defend free speech. <https://smex.org/lebanon-new-coalition-to-defend-free-speech/>

26. CIVICUS Monitor. (2023, 4 August). Authorities use the criminal justice system to harass journalists and activists. <https://monitor.civicus.org/explore/authorities-use-the-criminal-justice-system-to-harass-journalists-and-activists/>

27. Ismail, N. (2025). *Confronting structural silencing: Challenges and resistance among digital feminist activists in Lebanon*. SMEX. <https://smex.org/research-report-confronting-structural-silencing-challenges-and-resistance-among-digital-feminist-activists-in-lebanon/>

28. Ayyad, S. (2023, 5 April). Lebanon: Summoning Journalists in Beirut and Silencing Voices in Mount Lebanon. SMEX. <https://smex.org/lebanon-summoning-journalists-in-beirut-and-silencing-voices-in-mount-lebanon/>

29. SMEX. (2023, 17 July). Ruling against Sadek Sets Dangerous Precedent for Freedom of Opinion in Lebanon. <https://smex.org/ruling-against-sadek-sets-dangerous-precedent-for-freedom-of-opinion-in-lebanon/>

applications were circulating false information about the “unofficial” exchange rate between the dollar (USD) and the Lebanese lira (LL).³⁰

32. Statistics from SMEX’s Digital Safety Helpdesk show a concerning rise in cases of sexual blackmail, particularly targeting members of the LGBTQ+ community. Journalists and activists were the most prominent groups targeted over the 2021-2025 period. Targeted groups such as activists and journalists face exaggerated content moderation, censorship and obstacles that suppress their voices, including shadow bans, account suspensions and restrictions on electronic activities like live broadcasting, publishing and content accessibility.³¹
33. In most of the speech cases documented by members of the Coalition to Defend Freedom of Expression in Lebanon (of which SMEX is a founding member), the prosecution and security agencies acted improperly – and sometimes illegally – to intimidate and silence people charged in these cases. People interviewed by members of the Coalition described a range of physical and psychological interrogation tactics they believed were intended to humiliate, punish and deter them from publishing content deemed to be insulting to or critical of powerful people. Public prosecutors and interrogating agencies also pressure people to sign pledges promising not to write defamatory content about the complainant in the future or to remove their offending content immediately, before those accused appear before a court to present their defence and in some cases without bringing charges against them. However, these pledges have no legal bearing as they violate fundamental rights and freedoms.³²

Recommendations relating to freedom of expression online

34. End judicial harassment and criminal prosecution of journalists and activists through the use of repressive defamation laws, undue process and military tribunals aimed at restricting freedom of expression and press freedom.
35. Ensure due process and judicial integrity when summoning and interrogating journalists and other individuals.
36. Abolish articles criminalising libel, slander and defamation (including articles 292, 383-386, 388, 398, 474, 582 and 584 of the Penal Code), replacing them with civil defamation provisions that do not carry prison sentences.
37. Amend article 317 of the Penal Code to criminalise only statements that amount to incitement to discrimination, hostility or violence, using clear definitions aligned with the Rabat Plan of Action.
38. Ensure that any new media regulation, including the New Media Law, is in compliance with article 19 of the International Covenant on Civil and Political Rights (ICCPR).
39. Carry out gender impact and human rights impact assessments as part of the development of any new media regulation.

30. SMEX. (2020, 7 May). Lebanon Blocks Unofficial Exchange Rate Apps, Threatening Right to Access Information. <https://smex.org/lebanon-blocks-unofficial-exchange-rate-apps-threatening-right-to-access-information/>

31. SMEX. (2024, 16 July). Digital Safety Helpdesk Statistics: Rising Electronic Repression in the Region. <https://smex.org/digital-safety-helpdesk-statistics-rising-electronic-repression-in-the-region/>

32. SMEX. (2020, 13 July). Op. cit.

40. Investigate attacks, harassment or intimidation of journalists and human rights defenders and hold those responsible accountable.
41. Guarantee journalists' right to work freely, protect their sources and ensure their safety from both physical and legal threats.

VI. TFGBV faced by women human rights defenders

42. Systemic issues such as restrictive legislation, TFGBV – including online harassment, surveillance and censorship in Lebanon – and institutional gaps in digital inclusion disproportionately impact women human rights defenders (WHRDs).
43. In Lebanon, 80% of victims of digital violence (e.g. victims of tactics such as doxxing or the leaking of personal information to incite offline harm and hate speech, including smear campaigns and cyberstalking) are women.³³
44. TFGBV encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of ICTs, such as phones, the internet, social media platforms and email.³⁴ These forms of digital violence against women have resulted in, or are likely to result in, physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms, including their freedom of expression and their ability to participate in digital spaces.³⁵
45. Cases of digital violence have increased year on year since Lebanon's last UPR. In 2023, 650 digital violence cases were reported to SMEX's Digital Safety Helpdesk, 135 of which targeted women.³⁶ These mainly included cases of online harassment, blackmail, misinformation and account hacking. In the same year, the Digital Safety Helpdesk responded to 71 instances of online violence against women, with 40% of cases involving hacked social media accounts. This trend strongly indicates a rise in hacking that targets women's social media accounts.³⁷
46. In 2024 alone in Lebanon, SMEX's Digital Safety Helpdesk received 33 cases of sextortion, eight cases of account impersonation, five cases of blackmail, four cases of online harassment, two cases of theft, three cases related to intrusion attempts and two cases of doxxing.³⁸ According to research carried out by SMEX, digital violence is carried out with the use of highly organised and coordinated troll farms. Troll farms operate under strategic agendas, typically have financial backing and are capable of launching large-scale harassment campaigns.³⁹
47. In 2023, following protests dubbed "Freedom March", a video was circulated on social media platforms, such as Instagram, YouTube and X (formerly Twitter), doxxing a group of

33. Ayyad, S. (2024, 4 March). 80% of Women in Lebanon Face Digital Violence. SMEX. <https://smex.org/80-of-women-in-lebanon-face-digital-violence/>

34. Ibid.

35. Ibid.

36. Ismail, N. (2025). *Confronting Structural Silencing: Challenges and Resistance Among Digital Feminist Activists in Lebanon*. SMEX. <https://smex.org/research-report-confronting-structural-silencing-challenges-and-resistance-among-digital-feminist-activists-in-lebanon/>

37. Ibid.

38. <https://smex.org/helpdesk/>

39. Ismail, N. (2025). Op. cit.

feminist activists who participated in the protests by exposing personal details about their jobs, lives and addresses.⁴⁰ Judicial authorities have yet to take any steps towards holding the responsible parties accountable.

48. Impunity, a lack of trust in government agencies and legal and institutional gaps that include a lack of access to remedies are all factors mentioned in testimonies gathered by rights organisations that lead to documented self-censorship among WHRDs. Moreover, fear of judicial harassment results in activists avoiding discussions of corruption or gender equality.⁴¹ Research by SMEX has found that women journalists in Lebanon regularly practice self-censorship to mitigate safety risks.⁴²
49. Feminist activists face unique challenges due to algorithmic biases that marginalise their content and increase their risk of online harassment. Posts addressing sensitive topics such as gender equality and women's rights are often met with hostility, failures in content moderation disproportionately impact feminist activism in Lebanon and women and marginalised groups face heightened online abuse.⁴³
50. The experience of comedian Shaden Fakhri is one of many examples. After one of her sketches on Islam and religious figures was leaked and broadcasted online, Shaden was at the centre of a severe controversy. She faced a smear campaign, threats of violence and calls for her prosecution by prominent religious authorities. Her fears for her safety and the lack of support from the government forced her to leave the country to ensure her safety.⁴⁴

Recommendations related to TFGBV faced by WHRDs

51. Engage with specialists in TGBFV, including civil society organisations, victims, survivors and researchers, to ensure government approaches and remedies fully address the real needs of those who have been harmed by TGBFV.
52. Ensure existing laws on gender-based violence include aspects of technology-facilitated violence and engage with specialists in TGBFV, including civil society organisations, victims, survivors and researchers to increase the capacity of law enforcement authorities to address TFGBV through gender-sensitive digital security trainings.
53. Provide measures for redress and reparation for victims/survivors of TFGBV, with the support of civil society and independent institutions. Such measures should include forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition and offline protection, tailoring measures to the circumstances and the preferences of the victim.
54. Provide adequate funding and resources to ensure that victims/survivors of TGBFV have a variety of options when seeking support, including legal and non-legal responses. These responses should allow victims/survivors time to consider their options and should not require engagement with the legal system in all instances.
55. In collaboration with civil society organisations and academia, conduct regular public campaigns to raise awareness on TFGBV by ensuring broader understanding of TFGBV

40. Ibid.

41. Ibid.

42. Ibid.

43. Ibid.

44. L'Orient Today. (2024, 18 July). Comedian Shaden Fakhri leaves Lebanon after controversy over one of her shows. <https://today.lorientjour.com/article/1420712/comedian-shaden-fakhri-leaves-lebanon-after-religious-controversy-over-one-of-her-sketches.html>

and its impact, while highlighting key issues around digital security and safety. Support the National Commission for Lebanese Women to integrate these awareness-raising activities into the forthcoming National Action Plan for Women (2027-2030).

56. Exercise due diligence to prevent, investigate, prosecute and substantially address acts of gender-based violence, including those committed online or facilitated by technology, and to ensure access to justice and remedies and accountability for all responsible actors.
57. Ensure that legal frameworks adequately protect women's and gender-diverse people's freedom of expression (including political, religious and sexual expression), privacy and freedom from violence. Any restrictions to freedom of expression as a response to gender-based violence must be necessary and proportionate, should not be overly broad or vague in terms of what speech is restricted and should not over penalise (whether with respect to criminal sentencing or to responses that restrict internet or platform access).

VII. Marginalised groups

58. Marginalised groups in Lebanon include women, the LGBTQ+ community, migrant domestic workers, refugees and advocates for sexual and reproductive health and rights, all of whom frequently face heightened and disproportionate hostility and threats, including intensified hate speech and targeted harassment online.⁴⁵
59. Over the past five years (2020-2025), the Lebanese government's tightening restrictions on LGBTQ+ advocacy has intensified the climate of hostility towards people from the LGBTQ+ community. Targeted online harassment has led to offline consequences including blackmail, forced outings, family violence, arbitrary arrests and even physical violence by the country's Internal Security Forces (ISF).⁴⁶
60. This increasingly hostile rhetoric against these groups is also evident in the behaviour and attitudes of the authorities to protests against crackdowns on personal and political rights. At its third review, Lebanon accepted recommendations 150.142 and 150.147 to conduct investigations into the use of excessive force during protests and demonstrations.⁴⁷ Yet, these have not been implemented. For example, at the Freedom March on 30 September 2023, evidence reveals that the authorities failed to intervene as attackers threw stones and shouted homophobic slurs at protesters and physically assaulted them.⁴⁸
61. The lack of institutional protections, adequate support systems and protective mechanisms for activists impact the ability to address cyberbullying and online harassment and therefore impact freedom of expression, online and offline.⁴⁹
62. The failure of social media platforms to effectively address harmful content such as hate speech, cyberbullying and violent rhetoric, while disproportionately censoring the work and

45. Ismail, N. (2025). Op. cit.

46. Human Rights Watch. (2023). *"All This Terror Because of a Photo": Digital Targeting and its Offline Consequences for LGBT People in the Middle East and North Africa*. <https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt>

47. Human Rights Council. (2021). Op. cit.

48. Amnesty International. (2023, 3 October). Lebanon: Investigate assault on Freedom March protesters. <https://www.amnesty.org/en/latest/news/2023/10/lebanon-investigate-assault-on-freedom-march-protesters/>

49. Ismail, N. (2025). Op. cit.

voices of activists advocating for marginalised groups, limits the exercise of freedom of expression.⁵⁰ Arabic content is subject to excessive censoring as Meta's over-reliance on automated systems and insufficient investment in human content moderators severely hampers its ability to manage content effectively.⁵¹ This is particularly evident in the inconsistent handling of content relating to sexual and reproductive health rights.⁵² As identified under the United Nations Office of the High Commissioner for Human Rights' B-Tech project, states should implement a "smart-mix" of regulatory measures and policy incentives to protect against human rights harms related to the activities of technology companies. In doing so, they should be guided by deliberations involving civil society, affected groups, technology companies and other relevant stakeholders.⁵³

Recommendations related to marginalised groups

63. Take necessary steps to ensure the safety of marginalised groups, online and offline, and ensure adequate investigation into all attacks against activists, protestors, journalists, media professionals and marginalised groups.
64. Reform the legislative framework by passing legislation to prohibit discrimination based on sexual orientation or gender identity and repealing article 534 of the Penal Code.

VIII. General recommendations

65. Adopt explicit laws and policies aimed at strengthening protection from TFGBV for women and girls, in all their diversity.
66. Take all the necessary measures to protect and promote the civic space, online and offline, and ensure a safe and enabling environment for human rights defenders.
67. Ensure that human rights defenders, women's rights defenders and journalists are able to conduct their work and activities freely online and offline.
68. Encourage social media companies to communicate how they address their human rights impacts and consider introducing meaningful reporting and transparency standards to enhance understanding of the workings and risks to people related to digital technologies.

50. Ibid.

51. Ibid.

52. Ibid.

53. Office of the High Commissioner for Human Rights. (2021). *Bridging Governance Gaps in the Age of Technology: Key Characteristics of the State Duty to Protect*. United Nations. <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf>