MJRC
MEDIA&JOURNALISM RESEARCH CENTER

Maharat

Funded by the European Union
بتمويل من الاتحاد الأوروبي



POLICY BRIEF

Defining the Undefined Harm

AI-Generated Intimate Images and Cyber Blackmail in Lebanese Law

AUTHOR
Jad-Gui Shartouni

PUBLISHED
November 2026

POLICY BRIEF

Defining the Undefined Harm

AI-Generated Intimate Images and Cyber Blackmail in Lebanese Law

AUTHOR
Jad-Gui Shartouni

MJRC TEAM
Minna Aslama
Marius Dragomir
Adriana Mutu

MAHARAT TEAM
Maharat Foundation

PUBLISHED
November 2026

Lebanese law criminalizes blackmail and harassment in general terms — but defines no dedicated offense for a fabricated intimate image of an adult, leaving its creation without consent largely unaddressed.

> *"The laws reviewed do not specifically prohibit the non-consensual creation of a fabricated intimate image of an adult — even as the abuse targeting women grows."*

KEY FIGURES

99%

of deepfake-pornography subjects were female in 2023, and the number of deepfake videos identified online was up 550% since 2019 (Security Hero, 2023, as cited in Lazard et al., 2026).

80%

of reported digital-violence targets in Lebanon, 2020–2023, were women (SMEX, 2024).

5

structural gaps in current law — a three-tier reform agenda already drafted.

Executive Summary

Legislating ahead of further harm, for once

This brief asks whether Lebanese law can address a harm it has never named: an intimate image that is entirely fabricated, yet functions exactly like a real one in a blackmailer's hands. It combines doctrinal review, comparative analysis, and practitioner testimony to map Lebanon's current legal coverage against five structural gaps, and compares it with laws and proposals in five jurisdictions.

None of Lebanon's existing tools — the Penal Code (1943), Law 81/2018, or Law 205/2020 — were built with AI-generated imagery in mind. A dedicated draft law already exists: FEMALE convened judges, lawyers, and parliamentarians in 2025, now backed by a joint campaign with UNFPA (FEMALE, 2025a, 2025b, 2025c). What is missing is political movement, not a starting point.

The three-tier agenda that follows treats that movement as achievable: sequenced by cost and institutional capacity, not by ambition alone.

PROBLEM AT A GLANCE

01	No dedicated prohibition of synthetic intimate imagery of adults
02	No specific rapid-removal obligation
03	No dedicated civil action or emergency relief
04	Gaps in rapid protection and support
05	Enforcement limits vs. anonymous/foreign actors

SUGGESTED SOLUTIONS AT A GLANCE

Tier 1	Guidance, decentralization, training
Tier 2	Pass the drafted law; criminalize creation; build a removal clock
Tier 3	Civil remedy, victim fund, treaty accession, speech safeguards

METHODOLOGY

01
Doctrinal review of Lebanon's Penal Code, Law 81/2018, Law 205/2020, and published accounts of ISF practice.

02
Comparative analysis against the US, UK, EU, Spain, and Italy's synthetic-imagery frameworks.

03
Practitioner testimony: a semi-structured interview with a lawyer active in the FEMALE reform effort.

SECTION I

The Problem, and Why It Matters Now

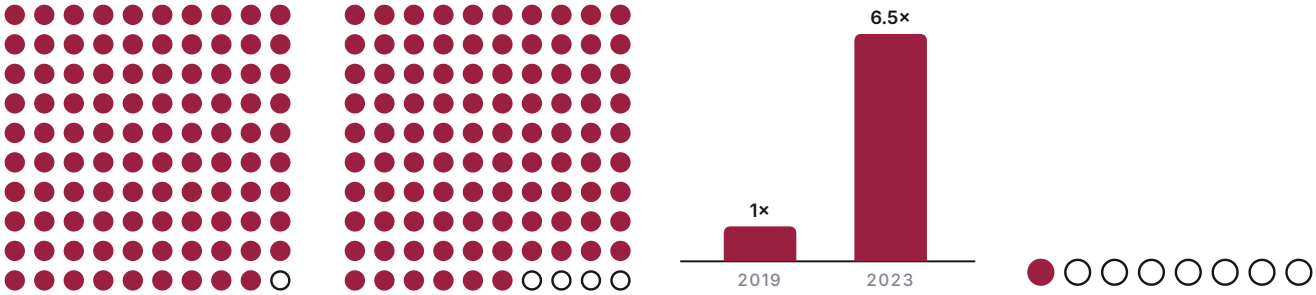
AI tools that generate photorealistic intimate images of real people, without any genuine intimate photograph, are now widely accessible and free. This is a growing form of a harm researchers have documented for a decade as technology-facilitated gender-based violence (TFGBV) and image-based sexual abuse — a body of law and criminology that has argued for treating non-consensual intimate imagery as a distinct criminal wrong, not an extension of obscenity law (Henry & Powell, 2018; McGlynn & Rackley, 2017; Citron & Franks, 2014).

The evidence is consistent across methods. Ninety-six percent of deepfake videos identified online in 2019 were pornographic, and every top deepfake-porn site targeted women exclusively (Ajder et al., 2019); by 2023 the number of deepfake videos identified online had grown by 550%, and 99% of those targeted in deepfake pornography were women (Security Hero, 2023, as cited in Lazard et al., 2026). A Thorn survey published in 2025, covering young people aged 13–20 in the US, found that 1 in 8 personally knew a deepfake-nude target and 1 in 17 had been targeted themselves (Thorn, 2025). Victims range from teenagers to sitting legislators and a European prime minister (Gozzi, 2024; Ocasio-Cortez, 2026; Thorn, 2025). A late-2025 survey of 641 women journalists, human rights defenders and other public communicators in 119 countries, published by UN Women in 2026, found that 6% had been targeted by deepfakes or other manipulated imagery, within a pattern of online violence that the report describes as often deliberate and coordinated, aiming to silence them (Posetti et al., 2026). Recent EU-level analysis reaches the same conclusion through doctrinal review: existing instruments were not written for content that requires no genuine intimate photograph (Rigotti et al., 2024; EIGE, 2022).

According to ISF statistics obtained by SMEX, 80% of Lebanon's reported digital-violence targets between 2020 and 2023 were women. An unnamed security source told SMEX that many complaints were filed by Lebanese women abroad facing digital blackmail (SMEX, 2024). The same source reported that 82 people were detained and charged with cybercrimes against women in 2022, and 71 in 2023 (SMEX, 2024). Underreporting compounds the problem: victims cite fear, guilt, or distrust of the system as reasons for not reporting (NCLW, 2023).

What distinguishes AI-enabled abuse structurally is that no original image needs to exist. A victim can know an image is false while it remains, to any observer, indistinguishable from real — breaking the evidentiary anchor most legal frameworks assume, and potentially inviting an argument unavailable in ordinary image-abuse cases: "no real photo, no privacy violation." This is best understood through Wardle and Derakhshan's (2017) information disorder framework. A deepfake intimate image is fabricated content deliberately created and shared to cause harm, which makes it disinformation, yet it is designed to function like malinformation, inflicting the same damage as the leak of a genuine private image. This is the standard the brief uses throughout for what "criminalizing synthetic imagery" should mean: targeting harmful, non-consensual use, not the underlying technology.

FIGURE 1 **The abuse is gendered and growing**



99%

of deepfake-pornography subjects were female

2023

96%

of deepfake videos identified online were pornographic

2019

+550%

deepfake videos identified online since 2019

2019 → 2023

1 in 8

young people in the US (aged 13–20) now knows a target personally

2025

Sources: Ajder et al. (2019); Security Hero (2023), as cited in Lazard et al. (2026); Thorn (2025). Filled dots show the share named; the bars index 2019 to 1.

SECTION II

What Lebanese Law Currently Covers

2.1

The Penal Code

Legislative Decree No. 340 of 1943 (as amended) addresses this conduct only indirectly. Article 650 criminalizes extortion by threat of exposure, Article 578 criminalizes threats of unjust harm, and Articles 582 and 584 cover defamation and insult. Because Article 650 targets the threat rather than the authenticity of the material, prosecutors may apply it to deepfake blackmail where its elements are met; but no provision of the Code specifically criminalizes the non-consensual creation of fabricated intimate imagery of adults (Republic of Lebanon, 1943; Zayat & Mnasri, 2024).

2.2

Law No. 81/2018

The Electronic Transactions and Personal Data law penalizes unauthorized processing and disclosure of personal data and creates offenses such as illegal access to and interference with data and systems, but does not define synthetic or AI-manipulated imagery as a covered category (Republic of Lebanon, 2018; Council of Europe, 2023). Article 120 also amended Penal Code Articles 535–536 on child sexual abuse material. Article 535 covers depictions of minors, including drawings and images, in real, artificial or simulated sexual activity; Article 536 punishes production even when no minor actually took part (Republic of Lebanon, 2018; Council of Europe, 2023, pp. 5–6). On their wording, these provisions cover wholly synthetic images and images made using a real child's face. The law does not explicitly name AI or deepfakes, and no court decision applying these provisions to such images was identified for this brief. The creation gap this brief identifies therefore concerns images of adults. Privacy International (2019) also criticized the law for weak safeguards and oversight.

2.3

Law No. 205/2020

Law 205/2020 on Criminalizing Sexual Harassment establishes both criminal penalties and, on paper, a victim-support fund. Article 5 also recognizes claims for psychological, moral or material damage. In practice, the fund does not appear to have been operationalized, and the law is silent on image-based abuse specifically (Republic of Lebanon, 2020; Diba, 2025). Human Rights Watch (2021) had warned that similar funds were delayed for years because implementing decrees were not issued, and identified gaps in civil remedies.

2.4

ISF Cybercrime Bureau

According to Ghadir Haidar, a Lebanese lawyer and FEMALE member interviewed for this brief, a single national bureau handles intake, investigation, and referral for the entire country. It has built real capacity within a narrow mandate, but one office cannot absorb a

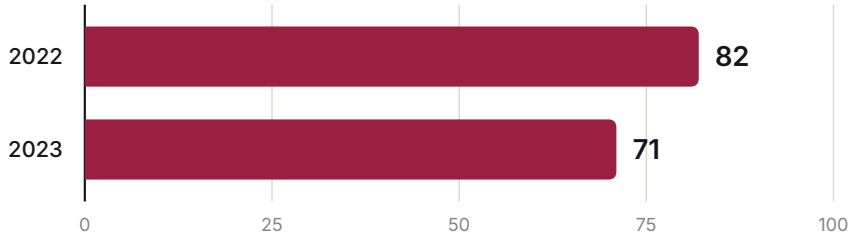
caseload with this geographic spread (G. Haidar, personal communication, July 22, 2026; Zayat & Mnasri, 2024). SMEX (2024) likewise quotes a source saying that poor infrastructure prevents the ISF's cyber bureau from keeping up with rising cases.

2.5

Jurisdiction and Cross-Border Reach

Lebanese courts have limited practical reach over anonymous or foreign-hosted perpetrators and platforms, and Lebanon is not party to the Budapest Convention, which could improve access to evidence across borders (Council of Europe, 2023).

FIGURE 2 **Individuals detained and charged, cybercrimes against women**



Source: SMEX (2024), quoting an unnamed security source.

SECTION III

What Lebanese Law Does Not Cover

1 **No dedicated prohibition of synthetic intimate imagery of adults** – The laws reviewed do not specifically criminalize the non-consensual creation of a fabricated intimate image of an adult, so prosecution must rest on associated conduct such as extortion or defamation – not on the image's existence.

2 **No specific rapid-removal obligation** – No law compels a platform or host to remove flagged content within a set window, so takedown often depends on voluntary compliance with each platform's own policy.

3 **No dedicated civil action or emergency relief** – Victims have no dedicated civil remedy for this abuse (general compensation rights, such as Article 5 of Law 205/2020, are not tailored to it) and no clear urgent-matters procedure to order removal before the underlying case is resolved.

4 **Gaps in rapid protection and support** – Neither a confidential, guardian-independent reporting path for minors nor a formal referral pathway linking a complaint to psychosocial or legal support is provided for in the laws reviewed.

5 **Enforcement limits against anonymous or foreign-hosted perpetrators** – Even where conduct could theoretically be charged, Lebanese courts have little practical reach over an anonymous account or a platform incorporated abroad. Absent treaty tools such as the Budapest Convention, this gap sits underneath all four gaps above – a law that fixes 1–4 domestically can still be evaded by moving the content, or the perpetrator, offshore.

SECTION IV

International Comparative Frameworks

UNITED STATES	TAKE IT DOWN Act (2025) criminalizes publishing non-consensual intimate imagery, including AI-generated content, and imposes a 48-hour platform removal clock upon a valid victim request, without prior judicial review, although requests must include a good-faith statement (U.S. Congress, 2025).
UNITED KINGDOM	Data (Use and Access) Act 2025, s.138 (in force since 6 February 2026; DLA Piper, 2026), criminalizes creation of, and now requesting creation of, non-consensual deepfake sexual images of adults in England and Wales — reaching the act before distribution. Platforms already have duties to act on illegal intimate-image content under the Online Safety Act 2023, and the Crime and Policing Act 2026 adds a 48-hour takedown provision for intimate images reported by the person depicted (commenced on 29 June 2026). Application to platforms depends on the relevant Ofcom codes completing the statutory process and coming into force (UK Parliament, 2026).
EUROPEAN UNION	The Digital Services Act requires hosting services to provide notice-and-action mechanisms and imposes systemic-risk duties on very large platforms; the Commission opened a DSA probe into X/Grok in January 2026 over risks from sexualized-image generation. Directive (EU) 2024/1385, which member states must transpose by 14 June 2027, requires criminalization of producing or manipulating intimate images and making them public without consent where serious harm is likely (European Union, 2022, 2024; European Commission, 2026).
SPAIN	The draft Organic Law on the Protection of Minors in Digital Environments, approved by the government in March 2025 (La Moncloa, 2025) and still before parliament as of September 2026 (Ochoa, 2026), would criminalize disseminating sexual or degrading deepfakes. It followed the 2023 Almendralejo case, in which schoolboys circulated AI-generated nude images of girls (Scottish Legal News, 2024). Separately, Article 17 of the existing Organic Law 8/2021 provides for personal reporting by children and confidential reporting channels (Kingdom of Spain, 2021).
ITALY	Law 132/2025 imposes severe criminal penalties (one to five years in prison) for disseminating, without consent, AI-generated or altered content that appears authentic and causes unjust harm; it was adopted after Prime Minister Meloni was herself targeted (Italian Republic, 2025; Gozzi, 2024).

TABLE 1 **Comparative Benchmark**

	US	UK	EU	SPAIN	ITALY	LEBANON
Principal instrument	TAKE IT DOWN Act	DUAA; OSA; Crime and Policing Act	DSA; Directive 2024/1385	Draft Organic Law (2025 proposal)	Law 132/2025	None dedicated
Synthetic imagery covered	Yes	Yes	Yes; due June 2027	Yes (draft)	Yes	None dedicated
Creation alone criminalized	No (distribution)	Yes; adults in England and Wales	No	No (dissemination; draft)	No (dissemination)	None dedicated
Platform removal duty	48-hour clock	Illegal-content duty; 48-hour provision	Notice-and-action; systemic duties	EU duties apply	EU duties apply	No specific deadline
Main limitation	No judicial gate on removal	Low charging rate (2025)	Requires capacity	Not yet enacted (Sept. 2026)	Dissemination only	No dedicated framework

Sources: U.S. Congress (2025); Online Safety Act 2023 (UK); Data (Use and Access) Act 2025 (UK); Crime and Policing Act 2026 (UK); European Commission (2026); European Union (2022, 2024); La Moncloa (2025); Ochoa (2026); Italian Republic (2025); UK Parliament (2026); Centre for Women's Justice et al. (2026); Rigotti et al. (2024); EIGE (2022). The comparison concerns the provisions discussed here; EU duties also apply in Spain and Italy. The UK charging data concern 2025 image-based abuse, before the 2026 creation offenses. For Lebanon, the creation gap concerns images of adults; the child-protection provisions are discussed in Section II, 2.2.

ANALYSIS

What Fits Lebanon, and What Does Not

No single framework transplants cleanly. Each was built for a state with enforcement capacity Lebanon does not have. The task is to borrow the design choices that survive weak institutions and discard those that presuppose strong ones.

ADOPT FOR LEBANON

US — the enforceable removal clock. A fixed takedown deadline is a rule a court can apply without technical sophistication. It matches a harm defined by speed of spread.

UK — criminalizing creation and request. Reaching the act before distribution closes off the "no real photo" argument at its root as a drafting choice, not a capacity one.

Spain — confidential reporting for minors. Article 17(1)–(2) of Spain's Organic Law 8/2021 permits children to report personally and requires confidential channels (Kingdom of Spain, 2021). Directly answers Lebanon's documented underreporting.

ADAPT WITH CAUTION / AVOID

EU — regulator-triggered systemic duties. Presupposes an audit body Lebanon lacks. Prioritize victim-triggered relief, which the DSA itself provides through notice-and-action, over regulator-led audits.

US — notice-based rapid takedown. Keep the clock, but pair it with judicial authorization — without it the over-removal risk can become a censorship tool.

Italy — penalty without reach. A severe sentence alone cannot remove foreign-hosted content. Criminalization is necessary but insufficient without cross-border reach.

> **The through-line:** the tiers that follow escalate deliberately, from measures that require no new statute to those that do — a responsive-regulation logic that matches intervention intensity to institutional capacity, and escalates only once lower-cost tools prove insufficient (Ayres & Braithwaite, 1992). The government does not need to assume capacity it does not have; it needs to build it in the sequence the evidence in Sections II–III already points to.

Three Design Principles

1 **Cover creation and request** — not only distribution, or the law arrives after the harm is complete.

2 **A binding removal clock** is worth more to victims than a severe penalty without one.

3 **Plan for implementation**, not only drafting: pair new offenses with training, investigative capacity and cross-border reach.

A Three-Tier Reform Agenda

This agenda does not begin from zero. In 2025, the NGO FEMALE convened judges, lawyers, and parliamentarians to draft Lebanon's first comprehensive cyber-violence law, now backed by a joint campaign with UNFPA (FEMALE, 2025a, 2025b, 2025c). The recommendations below are grounded in practitioner testimony from an interview conducted for this brief with Ms. Ghadir Haidar, a Lebanese lawyer and FEMALE member, and follow the escalating, capacity-matched logic set out above (Ayres & Braithwaite, 1992).

> *"In Lebanon, we do not have a dedicated law that specifically addresses cyber violence. We rely on other frameworks, the Penal Code and the Electronic Transactions Law. Technology evolves rapidly while these laws, particularly the Penal Code, are outdated and have not kept pace."*
>
> — Ghadir Haidar, Lawyer & FEMALE member (personal communication, July 22, 2026)

Tier 1

Immediate, No New Legislation

1.1 **Prosecutorial guidance.** The Public Prosecution should clarify, by circular, that Penal Code Article 650 and Law 205/2020 can apply to deepfake-related extortion or harassment where their elements are met — countering the "no real photo, no crime" argument at the charging stage.

1.2 **Decentralize cybercrime capacity.** Establish specialized cybercrime centers in every judicial district, in stages, starting with trained regional intake desks in existing ISF stations. FEMALE received 198 cases in 2023, and its executive director reports over 300 cyber-violence cases a month nationwide (FEMALE, 2025b); both figures underline the need for this expansion.

1.3 **Specialized training across the chain.** Police, judiciary, and civil society — covering synthetic-media identification, evidence preservation under Law 81/2018, and trauma-informed complaint handling. The UK's low charging rates for image-based abuse are the cautionary benchmark (Centre for Women's Justice et al., 2026).

> *"Lebanon has only one Cybercrime Bureau to handle cases from across the country. This is far from sufficient given the growing number of complaints."*
>
> — G. Haidar (personal communication, July 22, 2026)

Tier 2

Legislative Reform

2.1 **Adopt the dedicated cyber-violence law.** One that "comprehensively criminalizes all forms of cyber violence" with "clear legal definitions" (G. Haidar, personal communication, July 22, 2026). The FEMALE draft is the vehicle; Parliament should take up the draft and move it through committee.

2.2 **Criminalize synthetic intimate imagery.** Creation, request, and distribution — following the UK's structural choice with the US definitional approach ("digital forgery"). The offense targets non-consensual, harmful use, not the technology itself: this is the standard set out in Section I, which treats deepfake intimate images as disinformation designed to inflict the harm of malinformation (Wardle & Derakhshan, 2017). A distribution-only offense, as Italy shows, arrives after the harm is complete. If the FEMALE draft omits creation, it is the single most consequential amendment to add.

2.3 **A binding rapid-removal mechanism.** An urgent-relief procedure before an urgent-matters judge, granting removal and non-dissemination orders within days, independent of the criminal case — Lebanon's equivalent of the US 48-hour clock, adapted to issue removal orders to local hosts and targeted access-restriction orders to local ISPs and to support takedown requests to platforms under their own policies. Realistic for Lebanon specifically because it is scoped to what a Lebanese court can actually reach — local intermediaries, not foreign platforms directly — and because it is paired from the outset with 3.4's judicial-authorization safeguard, which is exactly what the unmediated US version lacks (Section IV, Table 1).

2.4 **Confidential reporting for minors.** Accessible without requiring a guardian's participation, modeled on Article 17(1)–(2) of Spain's Organic Law 8/2021. Girls and young women aged 12–20 were identified at FEMALE's October 2025 roundtable as the demographic most affected by reported cyber violence in Lebanon (FEMALE, 2025b), and children face particular risks from deepfakes (European Parliamentary Research Service, 2025).

"During those delays, harmful content may continue to spread online, causing further harm to the victim."

— G. Haidar, on the cost of ordinary criminal procedure (personal communication, July 22, 2026)

Tier 3

Structural

3.1 A dedicated standalone civil right of action with statutory damages, severing the victim's remedy from the criminal timeline.

3.2 Ensure an operational Law 205/2020 victim fund, with a mandate extended to cyber-violence victims and formal referral pathways.

3.3 Cross-border cooperation. Initiate the accession process to the Budapest Convention on Cybercrime (ETS No. 185) and align Lebanon's domestic legislation with its international cooperation and electronic evidence provisions. Without stronger international cooperation mechanisms, Lebanon's ability to investigate and prosecute cyber-violence offenses involving foreign-based perpetrators, platforms, or digital evidence remains constrained.

3.4

Free-expression safeguards from the outset — judicial authorization for every removal order, attested complaints, tightly drawn definitions. Adopt these safeguards together with the removal mechanism in 2.3. Without them, a law meant to protect women could be repurposed against speech. Lebanon's defamation provisions have already been used against peaceful critics (Human Rights Watch, 2019).

Closing Statement

The window to legislate ahead of further harm is open — and will not stay so.

Lebanese law does not adequately address fabricated intimate images. AI-generated intimate pictures expose that gap. Lebanon's laws carry five specific weaknesses that can still be exploited. Other countries tried to fix the same problem and made mistakes Lebanon can now avoid.

Spain's proposal followed the Almendralejo case. Italy legislated after its prime minister was targeted. The UK introduced significant legislative protections, yet continues to face serious enforcement shortcomings: a 2026 super-complaint about policing documented a charging rate of just 4.5% for image-based abuse offenses in 2025 across 39 police forces, alongside deficiencies in police training and investigative practice (Centre for Women's Justice et al., 2026; Dulieu, 2026). Lebanon, unusually, holds the position all of them would have preferred: a draft law already written, parliamentary champions engaged, and the chance to act before a scandal forces its hand.

TIER 1

Guidance, decentralization, and training — can begin now, subject to resources.

TIER 2

Pass the drafted law; criminalize creation; build a removal clock.

TIER 3

Civil remedy, victim fund, treaty accession, speech safeguards.

Works Cited

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The state of deepfakes: Landscape, threats, and impact. Deeptrace Labs.

Ayres, I., & Braithwaite, J. (1992). Responsive regulation: Transcending the deregulation debate. Oxford University Press.

Centre for Women's Justice, #NotYourPorn, & Leigh Day. (2026, October 7). Super-complaint launches over systemic failings to police image-based abuse. https://www.centreforwomensjustice.org.uk/updates/super-complaint-launches-over-systemic-failings-to-police-image-based-abuse

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49, 345–391.

Council of Europe. (2023, November 26). Cybercrime legislation – legislative profile: Lebanon. Octopus Cybercrime Community. https://rm.coe.int/lebanon-en/1680aef825

Crime and Policing Act 2026 (UK), c. 20, s. 100 (commenced on 29 June 2026 under S.I. 2026/689). https://www.legislation.gov.uk/ukpga/2026/20/section/100 Commencement regulations: https://www.legislation.gov.uk/uksi/2026/689/made

Data (Use and Access) Act 2025 (UK), s. 138. https://www.legislation.gov.uk/ukpga/2025/18/section/138

Diba, C. (2025, November 29). Criminalizing sexual harassment in Lebanon: Legal achievements and challenges. The Reform Monitor, Lebanese Center for Policy Studies. https://www.lcps-lebanon.org/en/articles/details/5006/monitor-%7C-criminalizing-sexual-harassment-in-lebanon-legal-achievements-and-challenges

DLA Piper. (2026, April 9). How the law is catching up with AI "deepfakes." https://www.dlapiper.com/insights/topics/algorithm-to-advantage/how-the-law-is-catching-up-with-ai-deepfakes

Dulieu, S. (2026, October 7). Super complaint launches over police 'revenge porn' failures. The Justice Gap. https://www.thejusticegap.com/super-complaint-launches-over-police-revenge-porn-failures/

European Commission. (2026, January 26). Commission investigates Grok and X's recommender systems under the DSA [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-investigates-grok-and-xs-recommender-systems-under-digital-services-act

European Institute for Gender Equality. (2022). Combating cyber violence against women and girls. Publications Office of the European Union.

European Parliamentary Research Service. (2025, July 3). Children and deepfakes [Briefing]. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775855

European Union. (2022). Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act), especially Articles 16 and 34–35. https://eur-lex.europa.eu/eli/reg/2022/2065

European Union. (2024). Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. https://eur-lex.europa.eu/eli/dir/2024/1385/oj

FEMALE. (2025a, July 31). FEMALE initiates work on the first-of-its-kind draft law for protection against online gender-based violence. https://www.fe-male.org/archives/15686

FEMALE. (2025b, October 2). A step toward legislation: FEMALE leads the call for Lebanon's first cyber violence law. https://www.fe-male.org/archives/15751

FEMALE. (2025c, December 3). FEMALE and UNFPA Lebanon launch joint campaign for landmark cyber-violence law. https://www.fe-male.org/archives/15742

Gozzi, L. (2024, March 20). Giorgia Meloni: Italian PM seeks damages over deepfake porn videos. BBC News. https://www.bbc.com/news/world-europe-68615474

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

Human Rights Watch. (2019, November 15). "There is a price to pay": The criminalization of peaceful speech in Lebanon. https://www.hrw.org/report/2019/11/15/there-price-pay/criminalization-peaceful-speech-lebanon

Human Rights Watch. (2021, March 5). Lebanon: Sexual harassment law missing key protections. https://www.hrw.org/news/2021/03/05/lebanon-sexual-harassment-law-missing-key-protections

Italian Republic. (2025). Law No. 132 of 23 September 2025 on artificial intelligence, Article 26, introducing Penal Code Article 612-quater. Gazzetta Ufficiale, No. 223, 25 September 2025. https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/sg

Kingdom of Spain. (2021). Organic Law 8/2021 of 4 June on comprehensive protection of children and adolescents against violence, Article 17. https://www.boe.es/eli/es/lo/2021/06/04/8

La Moncloa. (2025, March 25). The Government of Spain strengthens the protection of minors in digital environments [Council of Ministers summary]. https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/250325-rueda-de-prensa-ministros.aspx

Lazard, L., Capdevila, R., Turley, E. L., Gilfoyle, K., & Stavropoulou, N. (2026). Deepfake technology and gender-based violence: A scoping review. Trauma, Violence, & Abuse, 27(5), 2666–2681. https://doi.org/10.1177/15248380251384271

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534–561. https://doi.org/10.1093/ojls/gqw033

National Commission for Lebanese Women. (2023). Lebanon Gender Equality Barometer: Cyber extortion and cyber harassment. https://nclw.gov.lb/wp-content/uploads/2023/03/LGEB_Cyber-Extortion-and-Cyber-Harassment.pdf

Ocasio-Cortez, A. (2026, January 22). Ocasio-Cortez, Lee join House members and advocates in calling to pass DEFIANCE Act [Press release]. U.S. House of Representatives. https://ocasio-cortez.house.gov/media/press-releases/ocasio-cortez-lee-join-house-members-and-advocates-calling-pass-defiance-act

Ochoa, A. (2026, September 26). El Congreso retoma la ley que prohibiría las redes sociales a menores de 16 años: las claves del debate. Moncloa.com. https://www.moncloa.com/2026/09/26/ley-redes-sociales-menores-16-congreso-3438153/

Online Safety Act 2023 (UK), c. 50. https://www.legislation.gov.uk/ukpga/2023/50

Posetti, J., Williams, K., Hellmueller, L., Renaud, P., Shabbir, N., & Aboulez, N. (2026, April). Tipping point: Online violence impacts, manifestations and redress in the AI age. UN Women. https://www.icfj.org/sites/default/files/2026-05/UN%20Women%20Tipping%20Point%20AI%202026.pdf

Privacy International. (2019, January 27). State of privacy Lebanon. https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

Republic of Lebanon. (1943). Lebanese Penal Code (Legislative Decree No. 340 of 1943, as amended).

Republic of Lebanon. (2018). Law No. 81 of 2018 on Electronic Transactions and Personal Data.

Republic of Lebanon. (2020). Law No. 205 of 2020 on Criminalizing Sexual Harassment.

Rigotti, C., McGlynn, C., & Benning, F. (2024). Image-based sexual abuse and EU law: A critical analysis. German Law Journal, 25(9), 1472–1493. https://doi.org/10.1017/glj.2024.49

Scottish Legal News. (2024, July 10). Spain: Court punishes schoolboys for spreading AI deepfakes of girls. https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls

SMEX. (2024, March 4). 80% of women in Lebanon face digital violence. https://smex.org/80-of-women-in-lebanon-face-digital-violence/

Thorn. (2025). Deepfake nudes & young people. https://www.thorn.org/research/library/deepfake-nudes-and-young-people/

UK Parliament. (2026, July 20). Written answer HL1835 on commencement of section 100 of the Crime and Policing Act 2026. https://questions-statements.parliament.uk/written-questions/detail/2026-07-08/HL1835

U.S. Congress. (2025). TAKE IT DOWN Act, Pub. L. No. 119–12. https://www.govinfo.gov/content/pkg/PLAW-119publ12/html/PLAW-119publ12.htm

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.

Zayat, R., & Mnasri, A. (2024, March). Digital violence against women in Lebanon: Legal and institutional context. The SecDev Foundation. https://portal.salamatmena.org/wp-content/uploads/2024/06/Lebanon-DVAW-2024-legal-EN.pdf

METHODOLOGICAL NOTE ON CITATION

The interview with Ms. Ghadir Haidar is cited in-text only, per APA convention for personal communications (e.g., "G. Haidar, personal communication, July 22, 2026"), and does not appear in Works Cited, as personal communications are not recoverable by the reader. Haidar consented to being named and quoted. The interview was conducted in Arabic, and the author translated the quotations into English.

MJRC
MEDIA&JOURNALISM RESEARCH CENTER

Maharat

Funded by the European Union
بتمويل من الاتحاد الأوروبي

Media and Journalism Research Center

This policy brief is a joint publication of the Media and Journalism Research Center (MJRC) and Maharat Foundation.

LEGAL ADDRESS

Tartu mnt 67/1-13b, 10115,
Tallinn, Harju Maakond, Estonia

POSTAL ADDRESS

6 South Molton St, London,
W1K 5QF, United Kingdom

ACADEMIC COOPERATION

MJRC has a cooperation agreement with
Universidade de Santiago de Compostela (USC).

CONTACT

www.journalismresearch.org
mjrc@journalismresearch.org

MAHARAT FOUNDATION

www.maharatfoundation.org
info@maharatfoundation.org

COVER PHOTO

Photo by Alexander JT on Unsplash,
used under the Unsplash License.

ARTIFICIAL INTELLIGENCE (AI) DISCLOSURE STATEMENT

The author used AI for research and source retrieval, translation of Spanish-language material, and paraphrasing. The text of this policy brief is the author's own.

CITE THIS POLICY BRIEF

Shartouni, J.-G. (2026). *Defining the Undefined Harm: AI-generated intimate images and cyber blackmail in Lebanese law*. Media and Journalism Research Center and Maharat Foundation.

PUBLISHED BY

Media and Journalism Research Center (MJRC) and Maharat Foundation.

