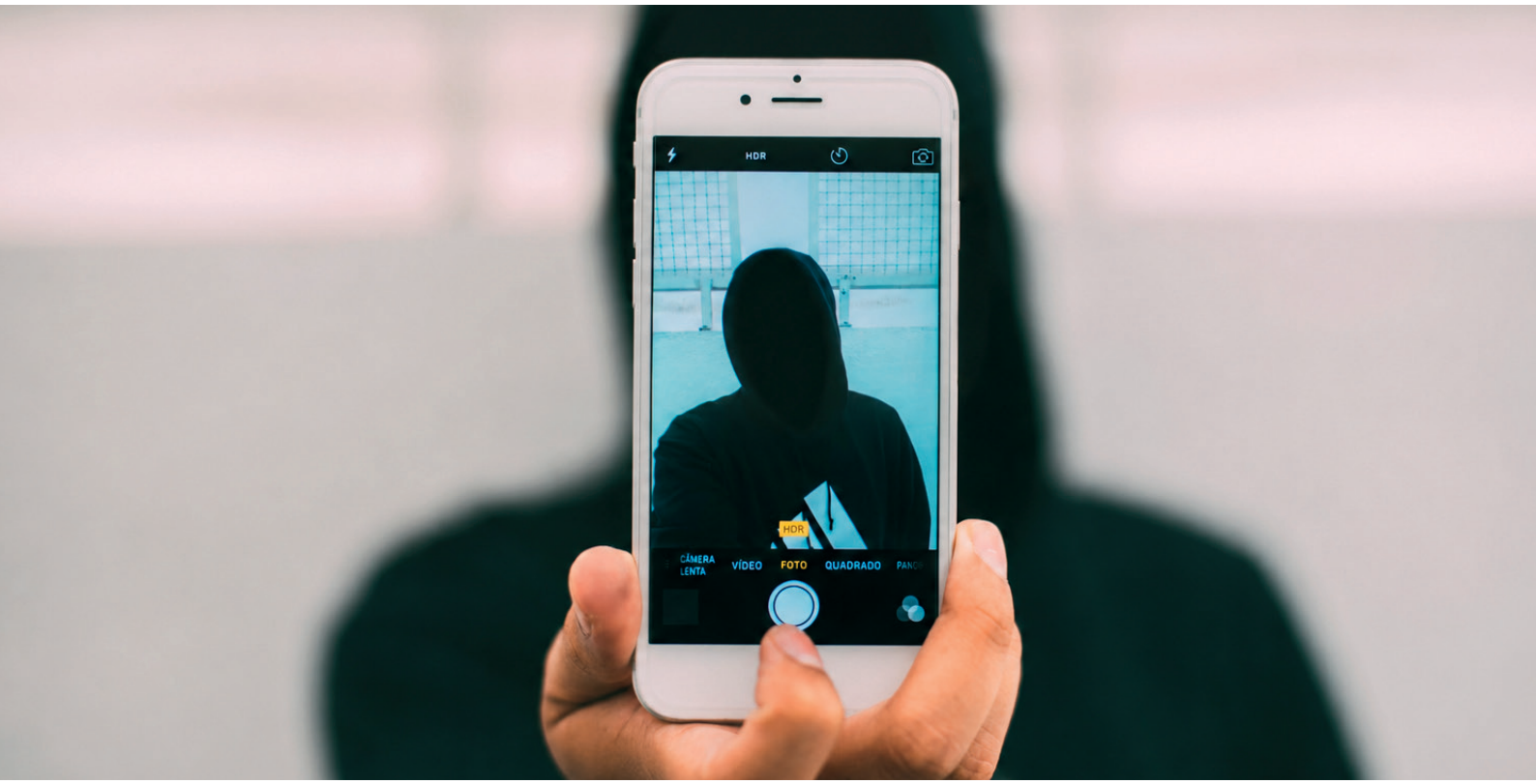
Inter-Parliamentary Union
For democracy. For everyone.

Combating non-consensual intimate imagery: A parliamentary action guide



Individuals can be targeted using non-intimate photographs taken from social media, websites and other online and public sources.

Executive summary

The rapid spread of generative artificial intelligence (AI) tools has triggered a surge in non-consensual intimate imagery (NCII), such as sexualized deepfakes. This trend disproportionately targets women and girls, including women parliamentarians. AI-generated NCII is a form of technology-facilitated gender-based violence (TFGBV) that affects the lives of millions of people and has a chilling effect across society.

According to UN Women, fewer than half of countries have laws covering online abuse, and even fewer have specifically addressed NCII.[1] As the capability of technology continues to evolve, parliaments worldwide are challenged to act in order to reduce these harms, uphold existing international obligations, establish the responsibilities of technology platforms, support individuals affected by NCII and hold offenders accountable.

The challenge of AI-generated NCII is one of the clearest, most high-profile tests of whether parliaments can shape the future of responsible AI.

1 UN Women, "When justice fails: Why women can't get protection from AI deepfake abuse" (26 February 2026).

This issue brief sets out five priorities for parliamentary action:

1. **Legislate to recognize AI-generated NCII as gender-based violence**, with technology-neutral definitions that cover creation, manipulation, possession, distribution, threatened distribution and commercialization.

2. **Ensure effective takedown and victim support mechanisms**, creating clear platform obligations including the rapid removal of NCII content, ensuring that police, prosecutors, schools and healthcare providers are equipped to respond, and fostering close collaboration between civil society organizations and platform providers to establish effective and meaningful protection for victims.

3. **Use oversight to track implementation, evidence and platform compliance** with legal frameworks and international obligations.

4. **Speak out publicly on NCII**, including launching prevention campaigns, raising awareness in society, building cross-party support in parliament and including the issue in national action plans around TFGBV.

5. **Cooperate internationally on a borderless harm** whose perpetrators, victims and distribution mechanisms can sit in different jurisdictions, including through the Inter-Parliamentary Union (IPU) and global AI governance processes.

The emergence of AI-generated NCII

The term "non-consensual intimate imagery" (NCII) refers to the creation, manipulation, possession, threatened and actual distribution of intimate material without the consent or against the will of the person depicted.[2]

This form of TFGBV disproportionately targets women and girls, including parliamentarians, political candidates, journalists, human rights defenders and other public figures. It poses urgent challenges to democratic institutions and human rights, forms part of a wider backlash against women's rights[3] and is structurally embedded within broader patterns of gender-based harm.[4]

The governance of AI is a question not only of technological innovation but also of democratic power: who sets the rules, who is protected and who is held to account. The pace at which these technologies are advancing, and the concentration of their development among a small number of global actors, together pose one of the defining policy challenges of the moment for democratic institutions.

Voluntary action by companies has so far fallen short of what is needed to prevent the creation and circulation of NCII at scale, and commercial incentives can pull in the opposite direction. Parliaments are uniquely positioned to close that gap, having driven the most consequential responses to date through their core functions: legislating, scrutinizing executive action and the companies behind these technologies, and speaking publicly on behalf of those affected. That work has placed political pressure on platforms, AI developers and governments to act. The examples set out in this issue brief are intended to support that work by showing what parliaments around the world have already done to shape this issue and what others can learn from their experience.

Defining the issue

Terminology and definitions vary across legal and policy contexts, with some jurisdictions referring to "sexualized deepfakes", "intimate deepfakes" or "deepfake pornography". This issue brief uses the term "non-consensual intimate imagery" (NCII), which centres the absence of consent while also encapsulating a broader range of abusive material. By focusing on "intimate" rather than just "sexually explicit" content, the term encompasses material such as clothed sexual acts and other degrading, violent, graphic or obscene depictions that narrower legal definitions might fail to address. While NCII is overwhelmingly pornographic, the specific use of "intimate" is intended to catch nude, sexualized, bodily private or degrading material without overextending to general private-life, family or romantic imagery, which raises distinct issues of defamation, harassment or disinformation.

Annex C contains references demonstrating how a selection of jurisdictions have defined the offence in law.

AI is transforming the scale of harm, forms of abuse, and range of actors involved in, or profiting from, NCII.[5] Recent years have witnessed a dramatic increase in AI-generated NCII, particularly sexualized "deepfakes".[6] High-profile cases involving public figures have significantly shaped societal debates on AI-generated NCII.[7]

Sexualized deepfakes predate the current wave of generative AI, but new tools have made it far easier to produce synthetic and manipulated sexualized images.[8] Today, individuals can be targeted using non-intimate photographs taken from social media accounts, messaging platforms, professional websites, campaign materials or other public sources. Capabilities that once required specialist software and technical knowledge are now widely accessible and available through consumer applications that require little to no expertise, helping move these capabilities from specialist communities into mass consumer use.

2 Government of the United Kingdom, "Crackdown on intimate image abuse as government strengthens online safety laws" (13 September 2024); Australian Government, Attorney-General's Department, "National statement of principles relating to the criminalisation of the non-consensual sharing of intimate images" (19 May 2017); Irish Statute Book, Harassment, Harmful Communications and Related Offences Act 2020, Section 2 (2020); UN Women, "When justice fails: Why women can't get protection from AI deepfake abuse" (26 February 2026).
3 United Nations, "Online 'manosphere' is moving misogyny to the mainstream" (7 March 2025).
4 Elisa Berlin and others, "Tackling Gender-Based Violence to Increase College Students' Well-Being: A Study on Psychosocial Dimensions Affecting Attitudes Toward the Nonconsensual Intimate Image Dissemination" (2024); UN Women, Tipping point: The chilling escalation of violence against women in the public sphere (2025).
5 UN Women, How AI is exacerbating technology-facilitated violence against women and girls (2025).
6 Asher Flynn and others, "Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery" (2025).
7 Julia Sturges, "Taylor Swift, Deepfakes, and the First Amendment: Changing the Legal Landscape for Victims of Non-Consensual Artificial Pornography" (2024).
8 UN Women, How AI is exacerbating technology-facilitated violence against women and girls (2025).

Research is beginning to grasp the breadth of the problem:

- NCII increasingly affects children and adolescents. A joint investigation published in April 2026 identified school-based NCII incidents across 28 countries.[9]
- The Internet Watch Foundation reports that a convincing deepfake of a specific person can be produced from around 20 photographs in 15 minutes.[10] Social media photos can therefore provide enough material to imitate a real person's face and likeness.
- These advances have resulted in a proliferation of web and app-based "nudification" and face-swap services. As early as September 2023, a sample of 34 such services was shown to be attracting 24 million unique visitors a month.[11]

These capabilities are combined with platform distribution and monetization systems. In fact, AI "undressing" services were already operating as scaled and monetized businesses in 2023, using affiliate marketing, spam tactics and mainstream platforms to reach users.[12]

Current systems are embedded in browser tools and mobile apps that remove the need for coding or specialist hardware. A user can now upload a photo, choose a preset and receive a sexualized synthetic image within seconds.

A high-profile case occurred in August 2025, when xAI launched Grok Imagine on its X platform with a "Spicy" preset, with reporters demonstrating that the system would generate non-consensual sexual images of individuals and public figures on first use.[13] A particular subject of controversy was the intentional minimization of restrictions on user prompts. This development prompted rapid regulatory action and demand for stronger legal obligations on providers of generative AI tools to prevent the creation and dissemination of NCII.[14]

In the United Kingdom, the Office of Communications (Ofcom) opened a formal investigation under the Online Safety Act in January 2026,[15] and the European Commission opened proceedings against X under the Digital Services Act later that same month.[16]

Parliamentarians speaking out

"They are not harmless images – they are weapons of abuse, disproportionately aimed at women and girls. And they are illegal."[17]
Ms. Liz Kendall, Member of the House of Commons, Secretary of State for Science, Innovation and Technology, United Kingdom, January 2026

"Sexual images without consent is not innovation. It's an act of violence, it's unacceptable, and it must be stopped."[18]
Ms. Arba Kokalari, Member of the European Parliament, February 2026

"This is unacceptable and gross misuse of an AI function … Our country cannot be a bystander to women's dignity being violated publicly and digitally with zero consequences under the garb of creativity and innovation."[19]
Ms. Priyanka Chaturvedi, Member of the Council of States, Member of the Parliamentary Standing Committee on Information Technology and Communication, India, January 2026

"This is unacceptable and possibly illegal sexual exploitation. It is sexual violence."[20]
Ms. Dominique O'Rourke, Member of the House of Commons, Canada, January 2026

"Punitive measures are key to address the misuse of AI for the creation and dissemination of sexualized deepfakes across society. It is key for parliaments to raise this issue and to increase protections of the ones most vulnerable, namely women and children."
Mr. Ernest Anim, Member of Parliament, Ghana, June 2026

The extent of the problem

UN Women reports a recent dramatic increase in NCII, particularly affecting women and girls,[21] with deepfake videos alone increasing by 550% between 2019 and 2023.[22] Data suggests the following:[23]

- Globally, 59.9% of women with internet access have personally experienced at least one form of TFGBV.[24]
- 98% of all deepfake videos circulating online are pornographic, and 99% of those targeted are women or girls.[25]
- Children are increasingly targeted. Over 20,000 AI-generated NCII images were identified on a single dark-web forum in one month in 2023.[26]

9 Matt Burgess, "The Deepfake Nudes Crisis in Schools Is Much Worse Than You Thought" (15 April 2026).
10 Internet Watch Foundation, Harm without limits: AI child sexual abuse material through the eyes of our Analysts (2026).
11 Santiago Lakatos, A Revealing Picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business (2023).
12 Santiago Lakatos, A Revealing Picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business (2023).
13 Jess Weatherbed, "Grok's 'spicy' video setting instantly made me Taylor Swift nude deepfakes" (5 August 2025).
14 Ramsha Jahangir, "Dutch Court Orders X, Grok to Stop AI-generated Sexual Abuse Content" (26 March 2026).
15 Office of Communications (Ofcom), "Ofcom launches investigation into X over Grok sexualised imagery" (12 January 2026).
16 European Commission, "Commission investigates Grok and X's recommender systems under the Digital Services Act" (26 January 2026).
17 Government of the United Kingdom, "Secretary of State statement to the House of Commons: 12 January 2026" (12 January 2026).
18 Owen Carpenter-Zehe, "Grok scandal prompts MEP move to ban non-consensual AI porn in new omnibus" (5 February 2026).
19 The Times of India, "Priyanka Chaturvedi writes to govt on AI abuse: Flags sexualisation of women; seeks urgent action" (2 January 2026).
20 Kate Bueckert, "Guelph MP pauses using X for social posts after Grok controversy" (24 January 2026).
21 UN Women, Repository of UN Women's work on technology-facilitated violence against women and girls (2025).
22 UN Women, "When justice fails: Why women can't get protection from AI deepfake abuse" (26 February 2026).
23 Maria Noemi Paradiso and others, "Image-Based Sexual Abuse Associated Factors: A Systematic Review" (2023).
24 Centre for International Governance Innovation (CIGI), Supporting a Safer Internet: Global Survey of Gender Based Violence Online (2023).
25 Security Hero, "2023 State of Deepfakes: Realities, Threats, and Impact" (2023).
26 Internet Watch Foundation, How AI is being abused to create child sexual abuse imagery (2023).

- In Canada, up to 28.5% of all undergraduate students have been impacted by NCII.[27]
- Gender and race shape victims' access to remedies and support in Australia, the United Kingdom and the United States of America, with disproportionate inequalities experienced by minority groups – underscoring the relevance of a response grounded in an intersectional understanding of gender-based violence.[28]

The harms of AI-generated NCII have been documented across the world. In the Republic of Korea, the August 2024 exposure of Telegram channels – including one with a reported 220,000 subscribers – distributing AI-generated sexual deepfakes of female students, teachers and soldiers triggered the National Assembly to amend the Sexual Violence Punishment Act in September 2024, raising maximum sentences to seven years and criminalizing possession and viewing.[29]

Spotlight on the Republic of Korea: Domestic legislation and its limits

The Republic of Korea has become one of the most significant cases of rapid legislative response to NCII, with parliament acting quickly and comprehensively following a sharp rise in abuse, including among students who created and circulated exploitative content using images of their peers.[30]

How parliament acted

In an interview with the IPU, Ms. Kim Nam-hee, member of the National Assembly of the Republic of Korea, described how the crisis had catalysed coordinated parliamentary action. A special parliamentary committee introduced reforms that expanded criminal liability beyond production and distribution to include possession and viewing of NCII.[31] Building on strengthened legislation on gender-based violence, adopted in 2024 with broad parliamentary consensus, victim protection mechanisms were reinforced – including faster content removal procedures and the formal establishment of support centres for those affected.[32] According to Ms. Kim Nam-hee, these reforms have already contributed to a measurable decline in the circulation of illegal deepfake content and to improved support for victims.

The case of the Republic of Korea nevertheless highlights the limits of domestic legislation when content is produced, hosted or distributed across borders. Platform accountability in particular remains a significant gap.

> "Even if a crime originates in one country but involves infrastructure or actors in another, it should not be treated as someone else's problem. Countries must work together closely to address these crimes effectively."
> Ms. Kim Nam-hee, Member of the National Assembly, Republic of Korea

What MPs can consider

- **Draw on international frameworks:** When making the case for domestic regulation of NCII, international instruments – including the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) – provide an established normative foundation.
- **Actively promote international agreements:** Parliaments can accelerate the negotiation, signing and ratification of relevant instruments, including the United Nations Convention on Cybercrime, to close the cross-border enforcement gaps that domestic legislation alone cannot address.

The impact of NCII on women and girls

The harms associated with NCII include anxiety, depression, shame, fear, social isolation, loss of income, educational disruption, and damage to relationships and professional standing, mirroring the impact of physical sexual abuse.[33] In some cases, NCII is linked to stalking, extortion, harassment, domestic abuse and other forms of coercive control,[34] with mental harm often intensified when offenders are former intimate partners or stalkers.[35] The process of seeking remedy can also lead to re-traumatization, as victims are often confronted with disbelief, lack of support or stigmatization.[36]

Many of the most serious cases arise in contexts defined by structural power imbalances, shaping both who is most at risk and how effectively the law can respond.

In addition, NCII often targets adolescents and girls.[37] Educational settings such as schools and universities involve both victims and perpetrators – and, where the perpetrators are children or adolescents, this raises specific questions about accountability and appropriate legal treatment.[38]

For women affected by human trafficking, domestic violence or conflict, or those from marginalized groups, the barriers to legal redress are compounded by pre-existing vulnerabilities. For instance, if a victim faces an insecure immigration status, or is at risk of deportation if they engage with law enforcement, NCII-related legislation may remain inaccessible in practice. The law therefore must account for the conditions under which abuse occurs. Otherwise, it risks failing those most at risk.

27 Maria Noemi Paradiso and others, "Image-Based Sexual Abuse Associated Factors: A Systematic Review" (2023).
28 Asia A. Eaton and others, "Perceptions of sexualized deepfake abuse across three nations: An exploration of how victim gender and race shape attitudes towards deepfake abuse in the United States, the United Kingdom, and Australia" (2026).
29 Heather Barr, "South Korea's Digital Sex Crime Deepfake Crisis" (29 August 2024).
30 Hyunsu Yim, "South Korea to criminalise watching or possessing sexually explicit deepfakes" (26 September 2024).
31 Shin Min-jung, "Korea passes bill making viewing non-consensual sexual deepfakes illegal" (27 September 2024).
32 Hyunsu Yim, "South Korea to criminalise watching or possessing sexually explicit deepfakes" (26 September 2024).
33 Clare McGlynn and others, "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse" (2020).
34 Telma Catarina Almeida and others, "Mental Health, Shame, and Resilience: A Study of Victims and Non-victims of Nonconsensual Intimate Image Sharing" (2025).
35 Kweilin T. Lucas, "Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology" (2022); Konstantinos Papachristou, Revenge Porn Helpline: 2023 Report (2023).
36 Brandon Sparks and others, "Where Is the Line? Perceptions of Victim Blame, Criminality, Harm, Morality and the use of Deepfake Nudifying Technology" (2026).
37 Matt Burgess, "The Deepfake Nudes Crisis in Schools Is Much Worse Than You Thought" (15 April 2026).
38 Ibid.

NCII and democratic processes

NCII has become a matter of increasing concern for democratic processes. The IPU has reported on gender-based violence within parliaments across the world.[39] Today, this threat is evolving with sexualized deepfakes disproportionately targeting women in public roles, creating a barrier to political participation and undermining the diversity of governing bodies.[40]

According to a 2025 report from UN Women, 70% of women in public life have experienced online violence, and 44% of women human rights defenders and 41% of women journalists have already experienced TFGBV, which includes NCII.[41] A subsequent UN Women study published in 2026 found that 41% of women journalists self-censored on social media to avoid being abused.[42]

Women parliamentarians are frequently targeted, and the European Parliamentary Research Service warns that deepfake tools are facilitating an increasingly hostile information environment for women in politics, with consequences for democratic participation both online and offline.[43] For legislators, advances in realism, speed, low-data personalization and mass distribution have outpaced laws designed for earlier forms of image-based abuse. In several jurisdictions, the impact on women MPs has been a catalyst for legislative action.

Spotlight on Germany: Prominent cases as drivers of parliamentary action

The German debate on NCII illustrates how high-profile individual cases can act as catalysts for parliamentary engagement. A prominent example concerns Ms. Collien Fernandes, an actress whose case significantly raised public awareness of NCII in Germany. Her husband was allegedly responsible for creating fake social media accounts in her name, which were used to disseminate manipulated intimate images over several years.

How parliament acted

Ms. Lena Gumnior, a member of the German Bundestag who has proposed legislation addressing AI-generated NCII, has emphasized that legal experts and professional associations have long identified regulatory gaps in addressing this form of digital abuse. A major emphasis of the draft law is its recognition of structural power asymmetries between perpetrators and victims. If the bill is passed, individuals who exploit women in vulnerable situations will be subject to more severe penalties.

"It is an inconvenient truth that public scandals are oftentimes the drivers of necessary change."
Ms. Lena Gumnior, Member of the German Bundestag

What MPs can consider

- **Identify legislative gaps early:** Parliamentarians should build on existing research and engage closely with legal experts throughout the process.
- **Anchor legislation on NCII in established legal conversations on the criminalization of sexual violence:** Alignment with generally accepted standards and the involvement of professional associations specializing in criminal law help secure broad consensus and align changes in criminal law with existing interpretations of constitutional law.
- **Complement criminal law with accompanying mechanisms:** Reporting hotlines, ombudsperson offices and protections for women without secure residence status are needed alongside the offence itself.

Victim-centred responses

The creation, dissemination and commercialization of NCII involve multiple actors across the digital ecosystem and span different legal domains including criminal law, data protection law, digital platform governance and legislation on sexual violence.[44] These challenges are intensified by the transnational nature of digital content dissemination, the rapid advancement of technological capacities and the accessibility of generative AI tools.[45]

Many countries have already established laws criminalizing image-based abuse, which is defined variously as "digital sexual violence", "NCII" or "revenge pornography". Existing legal responses are, however, often poorly adapted to AI-generated NCII,[46] on account of the following reasons and factors:

- **Legal uncertainty preventing meaningful protection:** Generative AI enables perpetrators to produce highly realistic sexualized content from entirely non-intimate source material. In jurisdictions where criminal law addresses only the distribution of NCII, this leaves the creation of synthetic content insufficiently covered and makes it more difficult for individuals to take legal action.[47]
- **Novel dissemination patterns:** Harmful content circulates via pornographic websites, social media platforms, encrypted messaging services, private groups and cloud storage, often across multiple jurisdictions, including some where removal mechanisms are weak or slow.
- **Different roles and responsibilities of actors:** Diverse actors across the digital ecosystem – such as social media platforms, app stores, AI providers, search engine providers and payment processors – bear different

39 IPU and Parliamentary Assembly of the Council of Europe (PACE), Sexism, harassment and violence against women in parliaments in Europe (2018); IPU and African Parliamentary Union, Sexism, harassment and violence against women in parliaments in Africa (2021); IPU, Commonwealth Parliamentary Association (CPA) and ASEAN Inter-Parliamentary Assembly (AIPA), Sexism, harassment and violence against women in parliaments in the Asia-Pacific region (2025).
40 Maria Pawelec and Mateusz Łabuz, Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action (2025).
41 UN Women, Tipping point: The chilling escalation of violence against women in the public sphere in the age of AI (2025).
42 UN Women, Tipping point: Online violence impacts, manifestations and redress in the AI age (2026).
43 Naja Bentzen, Women in the age of AI-enabled disinformation (2026).
44 Alena Birrer and Natascha Just, "What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape" (2024).
45 Karen Hao, "Deepfake porn is ruining women's lives. Now the law may finally ban it." (12 February 2021).
46 National Police Chiefs' Council (NPCC), "Police warn of rising threat from sexual deepfakes" (24 November 2025).
47 Karen Hao, "A horrifying new AI app swaps women into porn videos with a click" (13 September 2021).

responsibilities in preventing, mitigating and remedying NCII, according to their role in the harm cycle of NCII.

- **Wide variation in perpetrator motivation:** Perpetrators act for various reasons – out of pornographic interest, for harassment, humiliation, coercion or blackmail, or as part of misogynistic hate campaigns – making it difficult for legal frameworks built around specific criminal intent to respond adequately across all cases.[48]
- **Context of harm:** NCII occurs in various societal contexts – including schools, where its impact is particularly acute. Crucially, minors are often not just victims of this abuse, but also involved in creating and distributing NCII. Such dynamics demand age-appropriate legal and educational responses, including specialized support systems for children and adolescents affected by NCII as well as targeted awareness-raising and prevention initiatives.[49]

These legal gaps exist within a broader societal context that needs to be considered in the response to NCII:

- **NCII is part of a wider phenomenon of gender-based violence:** AI-generated NCII intersects with organized misogyny, backlash against women's rights, and the structural amplification of online abuse through social media algorithms and recommender systems.[50]
- **Public awareness remains critically low:** Surveys suggest that 17.5% of respondents have been involved in taking or sharing intimate images.[51] This points to a need for sustained public awareness alongside legislative action.

Explicit criminalization of AI-enabled NCII is essential to give legal certainty for victims and communicate to potential perpetrators that the creation and dissemination of such material carries legal consequences. However, international organizations, civil society groups and legal experts agree that regulatory gaps are significant and that enforcement across borders consistently falls short.[52]

In this context, civil society organizations have played a particularly important role, notably by establishing reporting mechanisms for affected individuals and by exerting pressure on platform providers to remove NCII content. According to data from the Revenge Porn Helpline in the United Kingdom, only 4% of people who report abuse through publicly available helplines also report it to the police[53] and, despite the scale of harm, prosecutions remain rare, platforms routinely fail to act and victims are often re-traumatized in the process of seeking help.[54]

There is broad expert consensus that criminalization, while necessary, must be accompanied by a wider regulatory and societal response,[55] including a victim-centred approach and a higher level of societal awareness.[56] Recommendations include the following:

- **Accessible legal remedies and effective enforcement,** including in cross-border contexts
- **Reliable content removal,** encompassing detection, identification, moderation and swift takedown procedures
- **Victim support** and the active prevention of re-traumatization
- **Preventive measures,** including public awareness campaigns to address gender inequality and educational initiatives to address the normalization of digital sexual violence
- **Continued investment in detection technologies** and digital forensic tools to support both enforcement and victim protection

Researchers also advocate for a clear distinction between general deepfake regulation and NCII-specific legislation, to address the issue without restricting legitimate uses of synthetic media.[57]

"Criminal law alone is insufficient. It should be complemented by additional institutional mechanisms, such as reporting systems and ombudsperson offices. Moreover, the enforcement of legal protections becomes difficult, if not impossible, when affected women obtain residence status only temporarily and are deported while legal proceedings are still ongoing."
Ms. Lena Gumnior, Member of the German Bundestag

Parliamentary roles and responsibilities

Parliaments across the world have responded to the harms associated with NCII through actions spanning lawmaking, oversight of how existing protections are enforced, and the exercise of their representative and budgetary functions to ground policy in lived experience and resource the institutions that respond. Because NCII sits at the intersection of women's rights, child protection, human rights, democratic resilience and platform accountability, it requires parliaments to draw on all of these functions in combination, not in sequence.

Lawmaking

The legislative task is to define the offence in a way that captures AI-generated and AI-altered material as well as authentic imagery, frame it as gender-based violence rather than generic cybercrime, and pair the offence with the other instruments – statutory takedown routes, platform obligations and victim support – that determine whether the law works in practice.

Parliamentary action on NCII does not start from a blank slate. CEDAW and the Convention on the Rights of the Child

48 Maria Pawelec and Mateusz Łabuz, Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action (2025).
49 Matt Burgess, "The Deepfake Nudes Crisis in Schools Is Much Worse Than You Thought" (15 April 2026).
50 UN Secretary-General, Intensification of efforts to eliminate all forms of violence against women and girls: Technology-facilitated violence against women and girls (2024).
51 Anastasia Powell and others, "Perpetration of Image-Based Sexual Abuse: Extent, Nature and Correlates in a Multi-Country Sample" (2022).
52 CIGI, Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa (2021).
53 Konstantinos Papachristou, Revenge Porn Helpline: 2023 Report (2023).
54 UN Women, "When justice fails: Why women can't get protection from AI deepfake abuse" (26 February 2026).
55 Maria Pawelec and Mateusz Łabuz, Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action (2025).
56 Becca Branum and Mi Yeon Kim, Rapid Response: Building Victim-Centered Reporting Processes for Non-Consensual Intimate Imagery (2025).
57 Maria Pawelec and Mateusz Łabuz, Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action (2025).

create binding obligations on the great majority of States to protect women and children from gender-based violence, including in digital and AI-mediated environments (see annex A).[58] Regional frameworks reinforce this picture, with the Council of Europe's Istanbul Convention setting standards for an integrated response of prosecution, prevention and victim protection, and the African Union Convention on Ending Violence Against Women and Girls providing a parallel benchmark. The UN Convention on Cybercrime, the Global Digital Compact, and recent statements by the UN Human Rights Council and the CEDAW Committee have reaffirmed that these obligations apply with equal force to AI-enabled NCII.

The examples that follow illustrate the range of legislative approaches that have been adopted.

In the **United States of America**, legislative action at both the state and federal levels includes California's 2024 ban on NCII[59] and the bipartisan TAKE IT DOWN Act, passed in May 2025, which prohibits the production and dissemination of deepfakes, introduces differentiated protections for adults and minors, and requires online platforms to remove such content within 48 hours of notification.[60]

In **New Zealand**, the Deepfake Digital Harm and Exploitation Bill was introduced in May 2025 to amend the Crimes Act and the Harmful Digital Communications Act.[61]

At the regional level, the **European Parliament** has shaped the digital governance architecture affecting NCII regulation, with influence extending beyond the EU: the Digital Services Act imposes obligations on online platforms to manage illegal and harmful content; the AI Act addresses synthetic media more broadly; and the Directive on Combating Violence Against Women and Domestic Violence[62] requires Member States to criminalize certain forms of gender-based violence and to establish dedicated victim support structures, including contact points and online reporting mechanisms. Parliamentary discussions indicate growing consensus to classify nudification applications as a prohibited practice under the AI Act.[63]

Discussion on the inclusion of NCII within prohibited AI practices has also gained traction in legislatures outside the EU. One example is the Artificial Intelligence Bill, introduced to the Parliament of **Kenya** in February 2026 by Senate member Ms. Karen Nyamu, which prohibits the "non-consensual use of personal images or likenesses in AI-generated harm."[64]

Spotlight on Mexico: Victim-led advocacy and an evolving legal framework

In Mexico, a campaign led by women who had themselves experienced digital abuse helped secure recognition of digital violence in domestic law, and parliament has continued to revise the framework as the technology has evolved.[65]

The adoption of the "Ley Olimpia" at the federal level in 2021 established "digital violence" as a legally recognized category and criminalized the non-consensual dissemination of intimate material. Subsequent parliamentary initiatives expanded the definition to explicitly include sexualized deepfakes and a range of related harms – digital stalking and harassment, online denigration, and identity theft – that disproportionately target women. Corresponding provisions in the Federal Penal Code enable criminal prosecution.[66]

The framework set penalties of three to six years' imprisonment, with aggravating factors where the perpetrator was in a relationship of trust with the victim, where the victim was a minor, where there was intent to profit, and where dissemination was at scale. It also created a right to reparation, an obligation on platforms to remove content within tight deadlines, and a requirement that perpetrators issue a public apology.

In 2024, parliament returned to the law to address AI-generated material specifically, extending sanctions to sexualized deepfakes and other synthetic or manipulated images, reflecting a broader shift towards treating AI-enabled abuse as a violation of human dignity and gender equality.[67] While evidence of its effectiveness is not yet available, the law has contributed to greater awareness of NCII and, more broadly, of gender-based violence in Mexican society.[68]

"Digital violence does not recognize borders. If we do not legislate in response to artificial intelligence, technology will advance faster than human rights – and that we cannot allow. The 'Ley Olimpia' has taught us that dignity does not end in the physical world; dignity must also be upheld in the digital world."
Ms. Marcela Guerra Castillo, Member of the Chamber of Deputies, Mexico

58 Committee on the Elimination of Discrimination against Women (CEDAW Committee) general recommendation No. 35 (2017) defines due diligence obligation for States and explicitly addresses technology-facilitated violence against women. The Committee has made clear that States may be held responsible for the actions of private actors, including technology companies and individuals. The recommendation further calls on States to ensure that legal definitions suffice in capturing novel forms of digital violence.
59 Governor's Office of California, "Governor Newsom signs bills to crack down on sexually explicit deepfakes & require AI watermarking" (19 September 2024).
60 U.S. Senate Committee on Commerce, Science, and Transportation, "Senate Unanimously Passes Cruz-Klobuchar Bill Stopping AI 'Revenge Porn'" (3 December 2024).
61 House of Representatives of New Zealand, Deepfake Digital Harm and Exploitation Bill (2026).
62 European Union (EU), Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (2024).
63 Frank Schräer, "EU committee backs ban on deepfake-capable AI systems – with exceptions" (19 March 2026).
64 Parliament of Kenya, The Artificial Intelligence Bill, 2026 (2026).
65 Leonardo Lugo V, "Adiós a los 'deepfakes' y extorsiones, endurecen la ley contra fraudes con IA" (4 November 2025).
66 Cámara de Diputados del H. Congreso de la Unión, "Iniciativa con proyecto de decreto por el que se adiciona un párrafo segundo al artículo 390 del Código Penal Federal" (10 November 2020).
67 See Marcela Guerra Castillo, Member of the Chamber of Deputies of Mexico, Statement to the IPU Standing Committee on Democracy and Human Rights, 152nd Assembly, Istanbul (2026).
68 Marcela Hernández Oropa and others, "Digital sexual violence against women in Mexico: role of the Olimpia Law in transforming underlying gender norms" (2024).

Spotlight on Australia: A dedicated criminal offence and a regulator with teeth

Australia has paired a federal criminal offence on deepfake sexual material with a civil regulator – the eSafety Commissioner – vested with takedown powers, illustrating the integrated approach this priority calls for. Momentum for action accelerated when people in positions of influence were themselves targeted, and parliament has played an active role both in passing domestic legislation and in scrutinizing the practices of social media platforms.

On 5 June 2024, Mr. Mark Dreyfus, a member of the House of Representatives and, at the time, the serving Attorney-General, introduced the Criminal Code Amendment (Deepfake Sexual Material) Bill into the House. The primary offence covers use of a carriage service to transmit sexual material depicting another adult without consent, with a maximum of six years' imprisonment; aggravated offences carry seven years where the offender is a repeat offender or created the material. The drafting is technology-neutral, applying whether the material is real, edited or fully synthetic.[69] The Senate Legal and Constitutional Affairs Legislation Committee examined drafting concerns, exceptions and the proportionality of the measures before reporting in support.[70]

Parliament has also used its oversight function to press platforms directly. The eSafety Commissioner's confrontation with X Corp. – which refused to comply with a content removal notice and challenged the Commissioner's jurisdiction in the Federal Court – illustrated both the reach and the limits of regulatory powers over global platforms, and the importance of coordinated parliamentary pressure across jurisdictions to close those gaps.[71]

"We need to deal with big tech, that is unanswerable at the moment. Technology companies are scared of the unity of parliamentarians."
Ms. Sharon Claydon, Member of the House of Representatives, Australia

Oversight and budget scrutiny

Parliamentary oversight is critical to gather evidence on the scale of the problem, to establish whether legal frameworks need amendment and to assess whether existing measures are adequately enforced. This is especially important given that only a small share of victims report the abuse to police, and that platforms can be slow or unresponsive in removing content.[72]

Parliamentary committees have a key role to play in scrutinizing how governments and regulators are implementing existing protections, including by holding platforms and technology companies to account for their role in the circulation of harmful content.

Several parliaments have used their oversight powers to press governments and regulators to act on AI-generated NCII, as highlighted in the IPU's "Parliamentary actions on AI policy" monthly bulletin:[73]

- In **Austria**, in March 2026, the parliamentary Committee for Equal Treatment Affairs discussed a resolution concerning the establishment of legal consequences for the distribution and creation of NCII. The resolution calls on the government to create a clear legal basis for criminal prosecution, targeting both the generation and distribution of deepfakes.
- In **Switzerland**, in September 2025, the National Council adopted a motion calling for a comprehensive national strategy to address the harmful use of manipulated images online, with a focus on personal rights, child and youth protection, and the prevention of sexual exploitation.
- In the **United Kingdom**, in January 2026, a debate on non-consensual sexual deepfakes was held in the House of Commons. The debate highlighted concern over cases involving AI-based social media tools that generate and disseminate such content, with MPs calling for strengthened platform accountability and swift action by regulators.

The budgetary function is closely linked. MPs scrutinizing the budget can assess whether legislative measures are matched by funding for the institutions that victims engage with: police units with the training and tools to investigate digital offences; prosecutors familiar with the evidentiary challenges of synthetic material; regulators with the capacity to act against non-compliant platforms; victim support organizations equipped to handle the specific harms of image-based abuse; and, where minors are affected, schools and healthcare providers prepared to respond.

Representation and public leadership

Parliamentarians form a bridge between constituents, representatives of affected groups, and government agencies. Their role in identifying harm, amplifying overlooked experiences and mobilizing political attention is especially important in relation to NCII, which is often hidden because of stigma and significantly underreported.

MPs have led cross-party campaigns, arranged parliamentary hearings, proposed legislation, and shaped how police, prosecutors and platforms understand the seriousness of the harm.

While women parliamentarians have often led parliamentary action on NCII, all MPs share a responsibility to address the harms. Male parliamentarians have been actively engaged in advocacy on NCII as well, and have co-led parliamentary initiatives alongside their female colleagues. One example is the joint motion introduced by Mr. Süleyman Zorba and Ms. Meri Disoski in the Austrian Parliament, which sought to close gaps in the protection of women from NCII.[74] Another is

69 Parliament of Australia, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024, inserting s 474.17AA into the Criminal Code Act 1995 (Cth) (2024).
70 Parliament of Australia, Senate Standing Committee on Legal and Constitutional Affairs, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 [Provisions] – REPORT - August 2024 (2024).
71 eSafety Commissioner, "Senate Standing Committee Opening Statement: Criminal Code Amendment (Deepfake Sexual Material) Bill 2024", statement by Ms. Julie Inman Grant (23 July 2024).
72 UN Women, How AI is exacerbating technology-facilitated violence against women and girls (2025).
73 IPU, "Parliamentary actions on AI policy" (accessed 7 June 2026).
74 National Council of Austria, Entschließungsantrag der Abgeordneten Süleyman Zorba, Meri Disoski, Freundinnen und Freunde betreffend Missbrauchs-Deepfakes bekämpfen - Gesetzeslücken schließen (2025).

the support from male parliamentarians for a bill criminalizing NCII in Germany.[75]

> "Male parliamentarians can play an important role in addressing this issue. The response to sexualized deepfakes should involve collaboration across genders and political perspectives, as well as the active engagement of male parliamentarians in this conversation."
> Ms. Lena Gumnior, Member of the German Bundestag

Spotlight on Austria: Building a coalition for action on NCII

Parliamentary action on NCII is often driven by individuals who have themselves been directly targeted. Following a televised debate on violence against women, Austrian parliamentarian Ms. Meri Disoski received an email containing pornographic deepfake images and videos depicting her. The case illustrates how individual experience can drive the debate on NCII legislation forward, but also how parliamentary progress can be slow even where harm is widely acknowledged. A key challenge has been establishing that NCII is not a matter of artistic expression or legitimate speech, but a violation of fundamental rights that causes concrete harm.

"I also want to underline that this is not only a technological problem, but also a political decision, if we protect women and others, such as children who are confronted and affected by this."
Ms. Meri Disoski, Member of the National Council, Austria

Three lessons emerge from the Austrian experience. First, a clear criminal definition of AI-generated NCII as a stand-alone offence creates the foundation on which removal mechanisms, victim support and platform accountability can be built. Second, building on previous legislation – in this case, earlier domestic laws on online hate, followed by responses to cyberflashing and now to AI-generated NCII – allows parliamentary support to consolidate over time. Third, legislative reform is likely to encounter political and institutional resistance: coalition-building and sustained media engagement, often around high-profile cases, have been needed to overcome resistance to legislative action.

75 German Bundestag, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Strafbarkeit bildbasierter sexualisierter Gewalt (2026).

Five priorities for parliamentary action

Priority 1. Legislate to recognize AI-generated NCII as gender-based violence

AI-generated NCII frequently falls between gaps in existing law. A clear, technology-neutral offence framed within gender-based violence law provides legal certainty for victims, signals seriousness to perpetrators, and aligns domestic law with international obligations under CEDAW[76] and the Beijing Declaration and Platform for Action.

Parliaments can consider the following actions:

- **Define the full scope of the harm,** covering creation, manipulation, possession, distribution, threatened distribution and commercialization – applying whether the material is real, edited or fully synthetic.
- **Map the legal gaps,** including in criminal law, family law, cybercrime law and data protection law, and consider whether deepfake imagery is excluded from intimate image laws drafted before the advent of generative AI.
- **Frame the offence within gender-based violence law,** aligning it with national strategies on violence against women and with international obligations.
- **Draft technology-neutral offences** so the law does not need to be re-drafted with every advance in AI tools.
- **Distinguish between different groups of victims.** Parliaments around the world increasingly acknowledge the different harms posed by AI to adults and children. Accordingly, sexualized deepfakes involving children are often subject to significantly higher legal penalties, stronger protective measures, specialized reporting and support mechanisms, and targeted awareness and prevention campaigns.
- **Use the legislative stage to widen the offence where needed.** Parliamentary amendments during second reading have, in several jurisdictions, broadened the scope of executive bills to cover non-sexual deepfakes, non-consensual digital replicas of voice and likeness, and other adjacent harms.
- **Listen to those on the front line,** including victim support organizations, police, school counsellors, women's shelters and digital safety helplines, who can identify whether the law is workable in practice.

Priority 2. Ensure effective takedown and victim support mechanisms

A criminal offence on its own does not remove the image, and prosecution can take years even where laws are in place. Parliamentary action is most effective when it pairs the law with the practical infrastructure – takedown, platform obligations and victim support – that determines whether the law works for victims in practice.

Parliaments can consider the following actions:

- **Establish a statutory route to compel removal** so that victims have a path to immediate removal of damaging content without waiting for the outcome of a criminal case.
- **Set clear and auditable obligations on platforms,** including statutory time limits for removal, transparent reporting on NCII reports received, evidence preservation, and cooperation with lawful investigations.
- **Place obligations on the providers of AI systems, not only on perpetrators.** Mandatory safety standards that require AI companies to prevent their products being used to generate deepfake abuse material are more likely to drive systemic change than offences targeting individual users alone.
- **Fund the front-line institutions that provide victims with access to remedies,** including police, prosecutors, schools, healthcare providers, helplines and women's shelters, and use the budget cycle to test whether legislation is matched by capacity to respond. Effective coordination among public authorities, private companies and civil society organizations is essential to ensure meaningful access to remedies for individuals affected by NCII.

Priority 3. Use oversight to track implementation, evidence and platform compliance

Even where laws are in place, implementation often falls short. Reporting rates among victims are low, prosecution rates are lower still, and platforms based outside a given jurisdiction may not respond to takedown requests within meaningful time frames. Parliamentary oversight is the principal mechanism through which the gap between law on the page and law in practice can be tracked and acted on.

Parliaments can consider the following actions:

- **Use focused committee inquiries.** A short, focused inquiry can strengthen drafting at the legislative stage, surface implementation failures once a law is in force, and bring evidence into the public domain. Consider a planned review one to two years after enactment.
- **Hold public hearings.** Public hearings have been used effectively in the Philippines, the Republic of Korea, the United Kingdom and the United States of America to bring police, regulators, platforms and victim support organizations on the record, surfacing implementation failures and platform non-compliance.
- **Open inquiries into platform compliance.** Where platforms operate notice-and-takedown systems under statute, parliamentary inquiries can establish whether they are meeting their statutory obligations on response time, reporting, and cooperation with investigations.
- **Coordinate across committees.** AI-generated NCII rarely sits within the remit of a single standing committee. Joint sessions or dedicated task forces can pool the expertise of judiciary, science and technology, gender equality, education and home affairs committees.

76 CEDAW Committee, General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (2017).

- **Request disaggregated data,** compelling government and platforms to provide information on case numbers, prosecution rates, takedown response times and investigation duration, disaggregated by sex, age, disability and other relevant factors.
- **Hear from victims directly** – including from MPs' staff and those in public-facing professions, as well as from those in high-risk environments such as schools and universities – and gather evidence in confidential or third-party formats where appropriate.

Priority 4. Speak out publicly on NCII

The most consequential parliamentary action on AI-generated NCII has typically depended on parliamentarians being willing to take a public position, work across party lines and connect the issue to lived constituent experience. Public statements by MPs shape how police, prosecutors and platforms understand the seriousness of the harm, while cross-party consensus reduces the political cost of acting and the risk of legislation being unwound at the next change of government.

Parliaments can consider the following actions:

- **Speak publicly in clear language,** challenging framings that minimize the harm because the imagery is "AI-generated" or "not real".
- **Reach out to groups at heightened risk,** including women in public-facing professions, journalists, candidates, women human rights defenders, LGBTIQ+ communities and minors.
- **Use constituency channels.** Direct engagement with victims and support organizations can supply evidence on enforcement gaps that no other channel can.
- **Speak up where colleagues are targeted.** Where parliamentarians themselves are subject to AI-generated NCII, cross-party solidarity has been one of the most powerful signals that the harm is unacceptable – while silence from colleagues is read as the opposite.
- **Audit risks within parliament,** assessing whether MPs, candidates, parliamentary staff or their families have been targeted. Provide training and clear reporting channels, recognizing that MPs' staff are often the first to encounter deepfake material directed at their MP.
- **Strengthen parliament as a gender-sensitive institution**:[77] Establish support mechanisms for MPs and staff who experience NCII; ensure that gender equality committees have an explicit mandate that covers NCII; integrate NCII into parliamentary codes of conduct and workplace safety policies; and engage male parliamentarians as active and visible champions of zero tolerance.
- **Frame the issue as a matter of democratic participation.** Where women candidates and elected representatives are deterred from public life, the harm extends beyond the individual to the integrity of representative institutions.
- **Involve other parliamentarians across gender and political party affiliation in your effort.** While women have often been the drivers of parliamentary action on NCII, male parliamentarians can support the effort by raising awareness, as well as by initiating and supporting legislation on NCII.

Priority 5. Cooperate internationally on a borderless harm

AI-generated NCII rarely respects national borders. Perpetrators, victims and the platforms that host the content are typically distributed across several jurisdictions, and the global technology companies that operate the underlying systems are difficult for any single parliament to hold to account. Continued exchange between parliaments – on legislative approaches, on implementation experience and on holding global technology companies to account – will remain essential.

Parliaments can consider the following actions:

- **Engage with treaty bodies,** including the CEDAW Committee and the UN Special Rapporteur on violence against women, to highlight AI-generated NCII in periodic reviews.
- **Use the IPU and regional parliamentary assemblies** as platforms for sharing legislative approaches, model legislation and committee evidence across jurisdictions.
- **Coordinate parliamentary questioning of global technology companies.** A unified front helps ensure that smaller jurisdictions are not ignored and reinforces parallel scrutiny under regimes such as the Online Safety Act in the United Kingdom, the TAKE IT DOWN Act in the United States of America, and the EU's Digital Services Act.[78]
- **Engage in international AI processes such as the Global Dialogue on AI Governance,** which present an opportunity to frame AI-generated NCII as a parliamentary concern and not merely a technical or regulatory question.

77 IPU, Plan of action for gender-sensitive parliaments (2017); IPU, Plan of action for gender parity in parliaments (2026).
78 Office of Communications (Ofcom), "Ofcom launches investigation into X over Grok sexualised imagery" (12 January 2026).

Conclusion

AI-generated NCII has developed on a scale and at a speed that existing legal frameworks were not designed to address. It harms society as a whole, with the impact borne most heavily by individual women and children. It deters women from public life and tests the capacity of parliaments to govern an area where technology is moving faster than the legislative cycle. The harms are widespread and likely to be underreported.

The cases in this issue brief show that decisive parliamentary action is both possible and effective. They also show that progress is uneven and can be contested, that legislation alone is rarely sufficient, and that the most effective responses combine parliaments' lawmaking, oversight, representative and budgetary functions in coordination.

Does your parliament need support to act on AI-generated NCII? Or do you have a good practice to showcase?

The IPU offers tailored support to help parliaments respond to AI-generated NCII, including comparative legislative analysis and peer learning between parliaments. It also provides a platform for sharing successful parliamentary action with a global audience.

Contact the IPU at ai-research@ipu.org for more information or to request a briefing for your parliament.

ANNEX

A. International and regional legal instruments

International (United Nations) instruments

- Convention on the Elimination of All Forms of Discrimination against Women (1979)
- Convention on the Rights of the Child (1989)
- Beijing Declaration and Platform for Action (1995)
- Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011)
- United Nations Convention against Cybercrime (2024)
  - See legal definition of CSAM: Art. 14: "Offences related to online child sexual abuse or child sexual exploitation material"
  - See legal definition of NCII: Art. 16: "Non-consensual dissemination of intimate images"
- Global Digital Compact (2024)

Regional instruments

- **African Union:**
  - Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol) (2003)
  - African Union Convention on Ending Violence Against Women and Girls (2025)
    - See Art. 5: "State Obligations on Ending Violence Against Women and Girls"
- **Council of Europe:**
  - Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) (2011)
  - Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (2024)

B. Recommendations, resolutions and reports of international organizations

UN committees and Special Rapporteurs

- **Committee on the Elimination of Discrimination against Women (CEDAW Committee):**
  - General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (2017)
  - General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration (2020)
- **Council of Europe,** "General Reports on GREVIO's activities" (various years)
- **UN Secretary-General,** Intensification of efforts to eliminate all forms of violence against women and girls: Technology-facilitated violence against women and girls (2024)
- **UN Special Rapporteur on violence against women and girls**, Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (2018)

UN agencies and bodies

- **United Nations Educational, Scientific and Cultural Organization (UNESCO):**
  - Recommendation on the Ethics of Artificial Intelligence (2021)
  - Synthetic content and its implications for AI policy: a primer (2024)
- **United Nations Human Rights Council,** Accelerating efforts to eliminate all forms of violence against women and girls: preventing and responding to all forms of violence against women and girls with disabilities – Resolution adopted by the Human Rights Council on 13 July 2021 (2021)
- **United Nations Children's Fund (UNICEF),** Artificial Intelligence and Child Sexual Abuse and Exploitation (2026)
- **UN Women:**
  - Repository of UN Women's work on technology-facilitated violence against women and girls (2025)
  - How AI is exacerbating technology-facilitated violence against women and girls (2025)
  - Tipping point: The chilling escalation of violence against women in the public sphere in the age of AI (2025)
  - "When justice fails: Why women can't get protection from AI deepfake abuse" (26 February 2026)
  - Tipping point: Online violence impacts, manifestations and redress in the AI age (2026)
  - Beijing Dashboard: Beijing+30 Action Agenda (2026)

Inter-Parliamentary Union

- Sexism, harassment and violence against women in parliaments in Europe (2018)
- Sexism, harassment and violence against women in parliaments in Africa (2021)
- *The impact of artificial intelligence on democracy, human rights and the rule of law* (resolution adopted by the 149th IPU Assembly) (2024)
- Sexism, harassment and violence against women in parliaments in the Asia-Pacific region (2025)
- Kuala Lumpur Declaration: Parliaments and responsible AI (2025)

C. Legislation on NCII around the world

Australia

- **Government of New South Wales,** Crimes Amendment (Intimate Images) Act 2017 No 29 (2017)
- **Parliament of Australia:**
  - Online Safety Act 2021 (Cth) No. 76 (2021)
    - See Part 6 for the legal definition of "Non-consensual sharing of intimate images"

– Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 (2024)
- See legal definition of NCII in section 474.17A

European Union

- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (2022)
  - See Art. 1: "Subject matter"
  - See Art. 18: "Notification of suspicions of criminal offences"
  - See Art. 20: "Internal complaint-handling system"
  - See Art. 23: "Measures and protection against misuse"
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (2024)
  - See legal definitions in Art. 5: "Prohibited AI practices"
  - See proposed inclusion of nudification apps in Art. 5(1)(l)
- Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (2024)
  - See legal definition in Art. 5: "Non-consensual sharing of intimate or manipulated material"
- Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime (2012)

Germany

- **German Bundestag,** Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Strafbarkeit bildbasierter sexualisierter Gewalt (2026)
  - See legal definitions in § 184k(1) and § 184k(2)

India

- **Government of India,** The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023) (2023)
  - See legal definition in Art. 77: "Voyeurism"
- **Ministry of Electronics and Information Technology,** Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (2021)
  - See relevant provisions on non-consensual sharing of images
  - See Part II: "Due Diligence by Intermediaries and Grievance Redressal Mechanism"

Kenya

- **Parliament of Kenya,** The Artificial Intelligence Bill, 2026 (2026)
  - See Art. 30(f): "Ethical guidelines"

Mexico

- **Ministry of the Interior**:
  - Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, en materia de Centros de Justicia para las Mujeres (Ley Olimpia) (2021)
- Decreto por el que se reforman y adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, en materia de Centros de Justicia para las Mujeresl (2023)

Republic of Korea

- **National Assembly of the Republic of Korea,** Special Act on the Punishment, etc. of Sexual Violence Crimes (enacted 2013, amended 2024) (2024)
  - See legal definition in 2.13 Art. 14-2: "Distribution of false images, etc."

Sri Lanka

- **Parliament of Sri Lanka,** Women Empowerment Act, No. 37 of 2024 (2024)

United Kingdom

- **Government of the United Kingdom**:
  - Criminal Justice and Courts Act 2015 (2015)
    - See sections 33 and 34: "Disclosing , or threatening to disclose, private sexual photographs and films with intent to cause distress" and "Meaning of 'disclose' and 'photograph or film'"
  - Online Safety Act 2023 (2023)
    - See legal definition in section 188: "Sharing or threatening to share intimate photograph or film"
- **UK Parliament,** Non-Consensual Sexually Explicit Images and Videos (Offences) Bill (2024)

United States of America

- **Congress of the United States of America,** TAKE IT DOWN Act (2025)
- **United States Department of Justice,** Violence Against Women Act of 1994 (VAWA) as amended (2026)
  - See relevant provisions on digital sexual abuse

D. National parliamentary reports, and reports and activities of statutory human rights bodies

Reports

- **European Parliamentary Research Service:**
  - Tackling deepfakes in European policy (2021)
  - Children and deepfakes (2025)
- **German Bundestag:**
  - Deepfakes: Straf- und zivilrechtliche Implikationen (2024)
  - Office of Technology Assessment, Technikfolgenabschätzung (TA): Rechtliche und gesellschaftliche Herausforderungen und Potenziale von Deepfakes (2026)

- **Parliament of Australia,** Senate Standing Committee on Legal and Constitutional Affairs, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 [Provisions] – REPORT - August 2024 (2024)
- **UK Parliament,** House of Commons Women and Equalities Committee, Tackling non-consensual intimate image abuse (2025)

Parliamentary hearings and motions

- **National Council of Austria,** Entschließungsantrag der Abgeordneten Süleyman Zorba, Meri Disoski, Freundinnen und Freunde betreffend Missbrauchs-Deepfakes bekämpfen - Gesetzeslücken schließen (2025)
- **Parliament of Australia,** Senate Standing Committee on Legal and Constitutional Affairs, Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 [Provisions] – REPORT - August 2024 (2024)
  See Appendix 2 – Public hearings
- **UK Parliament,** House of Commons Women and Equalities Committee:
  - "Oral evidence: Tackling non-consensual intimate image abuse, HC 336" (6 November 2024)
  - "Non-consensual intimate image abuse" (letter to the Criminal Injuries Compensation Authority (27 November 2024)
- **House of Representatives of the United States of America,** Committee on Oversight and Accountability, Addressing real harm done by deepfakes (hearing) (2024)
- **Senate of the United States of America,** Committee on the Judiciary, The good, the bad, and the ugly: AI-generated deepfakes in 2025 (hearing) (2025)

E. Studies and publications by civil society and academia

- **Branum, Becca, and Mi Yeon Kim,** Rapid Response: Building Victim-Centered Reporting Processes for Non-Consensual Intimate Imagery (2025)
- **Centre for International Governance Innovation (CIGI),** Supporting a Safer Internet: Global Survey of Gender Based Violence Online (2023)
- **ESET,** "Nearly two-thirds of women worry about being a victim of deepfake pornography, ESET UK Research reveals" (20 March 2024)
- **European Institute for Gender Equality (EIGE),** Combating Cyber Violence against Women and Girls (2022)
- **Internet Watch Foundation (IWF),** Harm without limits: AI child sexual abuse material through the eyes of our Analysts (2026)
- **Papachristou, Konstantinos,** Revenge Porn Helpline: 2023 Report (2023)
- **Pawelec, Maria, and Mateusz Łabuz,** Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action (2025)

This issue brief builds on the ongoing work of the IPU to address violence against women in politics[1] and to support parliamentary action on AI,[2] as well as on a range of examples from parliaments. It is intended to serve as a practical guide for victim-centred parliamentary action.

This issue brief has been prepared with the understanding that NCII is an evolving issue. The capabilities of the technology are changing quickly, the cases that drive public debate are unfolding in real time, and parliaments are continually adapting their legislative, oversight, representative and budgetary responses. Further updates will be provided on emerging responses across parliaments to the issues at hand, and readers are invited to share updates on actions they have taken so that the wider parliamentary community can continue to learn from their experience. Contributions can be sent to ai-research@ipu.org and will be collated and distributed through IPU channels.

1 Inter-Parliamentary Union (IPU), Sexism, harassment and violence against women in parliaments in the Asia-Pacific region (2025).
2 IPU, "Artificial intelligence" (accessed 7 June 2026).

This study was made possible thanks to the parliamentarians who generously volunteered their time to speak about their personal and, for some, deeply painful experiences. The IPU is extremely grateful for their openness and trust. The IPU would also like to express its sincere appreciation to Ms. Lena Gumnior, Ms. Meri Disoski, Ms. Sharon Claydon, Ms. Kim Nam-hee, Ms. Marcela Guerra Castillo and their teams for providing us with valuable insights and expertise on the parliamentary response to NCII.

This issue brief was coordinated by Dr. Alexander Kriebitz, with significant contributions from members of the AI Policy Team, including Alex Read and Youngjoon Yoon, under the leadership of Andy Richardson. This study would not have been feasible without the close support and dedication of the IPU Gender Team. The authors are especially grateful to Isabella Flisi and Zeina Hilal for their invaluable feedback, substantive contributions and sustained engagement throughout the project.

The IPU gratefully acknowledges the support of the Swedish International Development Cooperation Agency (Sida) for its support towards the production of this issue brief.

ISBN (print) 978-92-9142-994-3
ISBN (web) 978-92-9142-995-0
Inter-Parliamentary Union (IPU), Combating non-consensual intimate imagery: A parliamentary action guide. Issue brief. (IPU, June 2026).