Closing the Gaps: **Addressing AI-facilitated non-consensual intimate images in Canada and Mexico.** A comparative diagnosis.

Authors: **Daniela Rojas** and **Claudia Del Pozo**
Contributors: **Nicté Cabañas and Amélie Côté**

October 2026



IVADO

EON INSTITUTE

with the support of

CANADA FIRST RESEARCH EXCELLENCE FUND

APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE

Acknowledgements

The authors express sincere thanks to all those who contributed to this project by participating in the interviews in both countries. The participants' time and invaluable insights, which were key in shaping this brief, are deeply appreciated. Their names are listed below in alphabetical order.

Elizabeth Avendaño, lawyer and feminist activist, Luchadoras

Senator Luis Donaldo Colosio, President, Digital Rights Commission, Senate of Mexico

Sarah Crawford, Executive Director, Canadian Resource Centre for Victims of Crime

Elise Dupras, Juvenile Delinquency Intervention Specialist and School-Based Cyber Counsellor, Marguerite-Bourgeoys School Board

Marcela Hernández, Co-founder, Defensoras Digitales

Floretta Mayerson, Co-founder, Violetta

Paola Ricaurte Quijano, Research Professor, Tecnológico de Monterrey

Catherine Régis, Professor of Law, Université de Montréal

Teresa Scassa, Research Professor, University of Ottawa

The statements in the report do not necessarily reflect the views of the experts consulted, but remain those of the report's authors.

This document was made possible through a collaboration between Eon Institute in Mexico and IVADO in Canada. Eon Institute is a Mexican think tank working across Latin America to foster more resilient societies in the age of AI through applied research, capacity building, and collaboration, connecting evidence and stakeholders to develop better policies and strategies. IVADO is an interdisciplinary, cross-sectoral research and knowledge mobilization consortium led by Université de Montréal whose mission is to develop and promote a robust, reasoning and responsible AI.

TABLE OF CONTENTS

03 **Key takeaways**

04 **Introduction**

05 **Individual and social impacts of AI-facilitated NCII**

05 **The role of tech companies across the harm chain of AI-facilitated NCII**

07 **General overview of regulatory frameworks and public policy worldwide**

07 Common trends in the regulation of NCII

09 Common trends in the regulation of CSAM

10 United States: The TAKE IT DOWN Act and beyond

11 **Country profile: Canada**

11 Overview of NCII abuse in Canada

12 Regulatory framework

13 Complaint and redress mechanisms

13 Regulatory, implementation, and coordination gaps

14 **Country profile: Mexico**

14 Overview of NCII abuse in Mexico

15 Regulatory framework

16 Complaint and redress mechanisms

16 Regulatory, implementation, and coordination gaps

17 **Key comparative findings**

19 **Public policy recommendations**

19 Cross-cutting policy recommendations

20 Specific recommendations for Canada

21 Specific recommendations for Mexico

22 **Conclusion**

22 **Notes**

KEY TAKEAWAYS

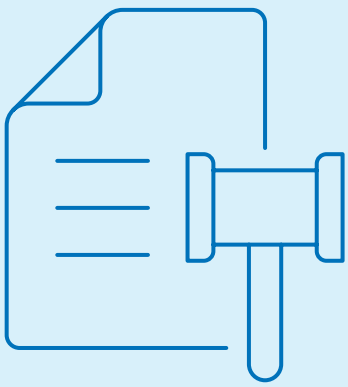
This report examines how Canada and Mexico are responding to AI-facilitated non-consensual intimate images (NCII), identifying structural gaps in prevention, redress and accountability. Despite operating from very different legal traditions and institutional contexts, both countries face the same underlying challenges.

What we found

- → Legal frameworks exist, but do not translate into justice. In Mexico, only 0.5% of NCII complaints reach the judiciary. In Canada, civil protections vary considerably depending on the province in which survivors reside, while protections under the *Criminal Code* were just strengthened in June 2026, and their application will require further study.
- → Institutional capacity is the main bottleneck. Prosecutors, judges and law enforcement officers lack both the technical training and the gender-sensitive perspective needed to effectively investigate and prosecute these cases.
- → Digital platforms operate without binding obligations. In June 2026, the Government of Canada introduced Bill-34 to impose new regulatory obligations on them. In October 2026, Mexico strengthened the protection of minors, without specifying the procedures for implementation or providing for any sanctions. In addition, most players are based in the U.S., and the Digital Trade chapter of the Canada–United States–Mexico Agreement (CUSMA) limits both the Canadian and Mexican governments' ability to hold them accountable.
- → Those most affected (members of Indigenous communities, racialized women and minors) have the least access to justice due to compounding barriers.

What we recommend

- → For both countries: coordinate a joint position in the upcoming CUSMA review to establish minimum platform accountability standards.
- → For Canada: prioritize the implementation of the new measures enacted under the Protecting Victims Act (Bill C-16, passed in June 2026); prioritize the adoption of Bill C-34, the Safe Social Media Act (introduced in June 2026); and expand emergency remedy mechanisms to all provinces.
- → For Mexico: Focus on implementing the existing Ley Olimpia framework before pursuing new legislation, and develop binding national protocols for prosecutors along with a single reporting pathway for survivors.



INTRODUCTION

The recent widespread deployment of artificial intelligence (AI) tools has not created digital gender-based violence, but it has fundamentally transformed it. Generative AI has lowered the barriers to producing and disseminating non-consensual intimate images (NCII), requiring minimal technical skills and cost on the part of perpetrators and lowering their risk of accountability, and ultimately fueling a faster, more accessible form of technology-facilitated gender-based violence.

The scale of the phenomenon is striking. By 2023, 98% of all deepfake videos online were non-consensual, and 99% of them depicted women.[1] The case of Grok (X's large language model) illustrates this phenomenon: in early 2026, it was used to generate approximately 1.8 million sexualized images of women in just nine days,[2] which corresponds to two images every second. This violence is not confined to adults. The same case also revealed child sexual abuse material (CSAM) involving girls aged 11–13.[3] In fact, reports of AI-facilitated CSAM increased by 1,325% between 2023 and 2024,[4] with a 2025 study across eleven countries finding that at least 1.2 million children had their images manipulated into sexually explicit deepfakes.[5] Additionally, the Internet Watch Foundation (IWF) reported 3,440 AI-facilitated CSAM videos in 2025, compared to just 13 the year before.[6]

Despite growing evidence of the emotional, economic, social and democratic consequences of AI-facilitated NCII, policy responses remain inadequate. By 2023, only one-third of economies had laws protecting women against cyber harassment, including Canada and Mexico,[7] and even when such legislation exists, enforcement is weak.

Canada and Mexico offer a particularly instructive comparative lens. Both navigate the complexities of federal systems while grappling with U.S.-based digital platforms that largely fall outside their regulatory reach, in addition to limited enforcement capacity and underfunded survivor-support systems. This report examines how Canada and Mexico are responding to AI-facilitated NCII, identifying structural gaps in prevention, redress and accountability across both contexts, and proposes concrete policy recommendations addressed to policymakers in both countries.

Limitation of the methodology

The methodology of this study draws on a qualitative, comparative and interdisciplinary approach combining documentary analysis, including regulatory frameworks, court rulings, civil society documents and academic literature, using nine semi-structured interviews conducted between February and March 2026 with experts from civil society, academia, legal practice and public institutions in both countries. The interview sample was intentionally targeted, but is not exhaustive of either ecosystem. While the Canadian sample does not include a legislative voice, other interviewees have engaged directly with legislative issues through research, contributions to official reports and public policy collaborations.

INDIVIDUAL AND SOCIAL IMPACTS OF AI-FACILITATED NON-CONSENSUAL INTIMATE IMAGES

Digital spaces have become a primary arena for gender-based violence. Rather than just extensions of offline harm, they operate as environments with their own dynamics, tools and power structures, where established forms of violence find new instruments.

A common misconception shaping institutional responses is that the synthetic nature of AI-facilitated NCII causes less harm. Evidence suggests otherwise: survivors experience chronic stress, anxiety, depression and erosion of self-worth, and some victims commit suicide,[8] comparable with what is experienced by survivors of non-synthetic NCII.[9] These consequences expand to professional and academic life, damaging reputations as well as disrupting attendance, concentration and academic development.[10] Survivors often lack accessible legal or technical options to limit the harm.

The gendered dimension of this harm extends beyond individuals to produce broader social consequences. Acting as a form of systematic social control, the normalization of AI-facilitated NCII reinforces the objectification of women, intensifies harassment and deters participation in public life.[11] When used against women politicians, journalists, activists and candidates, synthetic sexualized content can become a tool of political violence, silencing voices, undermining credibility and discouraging leadership.[12] For instance, Mexico's 2024 elections saw 217 women withdraw their candidacies due to pressure, threats or coercion, with formal complaints remaining rare due to intimidation and limited awareness of reporting mechanisms.[13]

It is important to note that these harms are not inevitable consequences of technological progress. They are the result of specific design choices, regulatory gaps, institutional limitations and insufficient accountability from tech companies.

THE ROLE OF TECH COMPANIES ACROSS THE HARM CHAIN OF AI-FACILITATED NON-CONSENSUAL INTIMATE IMAGES

AI-facilitated NCII harm emerges from an interconnected ecosystem of actors that operate at different stages of the harm chain. At the creation level, there are both the AI nudification apps and the misused generative AI platforms, and at the amplification level, there are the social media and content platforms where violence unfolds and is amplified. Chart 1 illustrates the different stages of the harm chain.

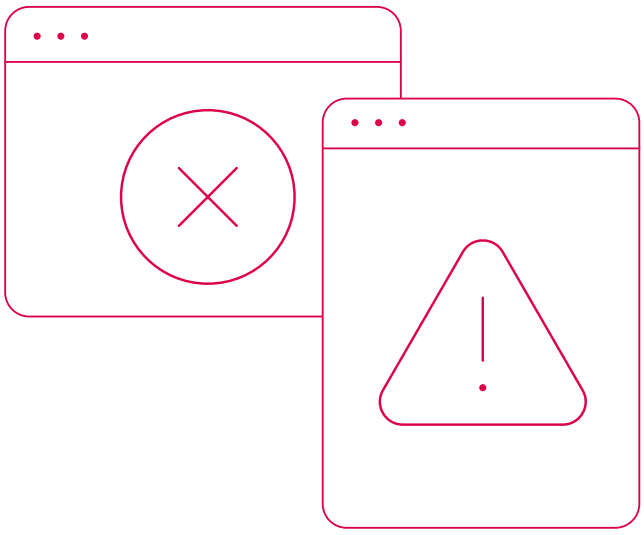
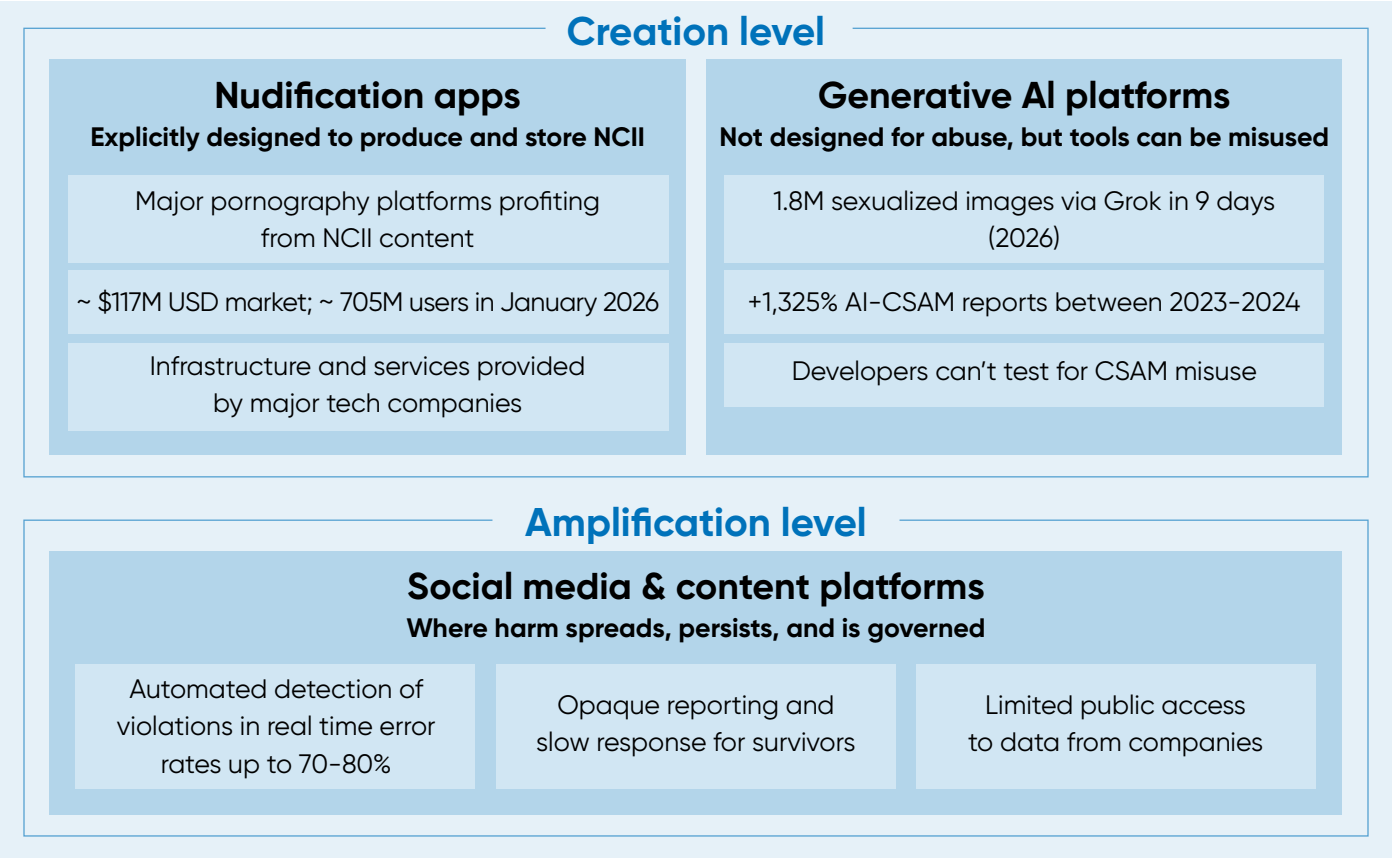


Chart 1: Harm chain of AI-facilitated NCII



At the creation level, many platforms—known as AI-powered nudification apps—are explicitly designed to produce and host NCII.[14] AI-powered nudification apps have become a highly profitable business. In January 2026, the Tech Transparency Project estimated the market at approximately 117 million US dollars and 705 million AI-powered nudification app downloads. Many of them using the infrastructure and services offered by major tech companies.[15] Two major cloud providers supply hosting and content delivery infrastructure for 62 of 85 nudifier sites.[16] Generative AI platforms also pose challenges, as they can be misused to create NCII and CSAM, a risk that developers cannot directly test given the illegality of processing such material.[17] In response, the U.K. authorizes a limited number of vetted organizations to test AI models under strict conditions.[18]

At the amplification level, social media and content platforms establish the rules governing behavior, content moderation and enforcement. While many of them use AI systems to detect violations in real time, the issue is not only that content moderation fails, reaching error rates of up to 70–80%,[19] but that human moderators receive labels or flags without sufficient context to act appropriately.[20] Furthermore, survivors report insufficient platform responses involving prolonged response times, opaque reporting processes and limited follow-up.[21]

Additionally, the extent of the problem is obscured by systemic opacity from these platforms, which tightly control access to information for the public, researchers, civil society organizations and policymakers. That said, some major social media companies have begun to acknowledge their role, with platforms like Meta partnering with civil society initiatives like StopNCII.org[22] and Take It Down[23] to facilitate the removal of NCII. They have also introduced stricter policies prohibiting both traditional and AI-facilitated NCII.[24]

In response to these challenges, recent years have seen a shift from blaming individuals who share NCII toward holding platforms directly accountable. Recent lawsuits provide early evidence of this shift. Key cases include France's legal action against Telegram for complicity in illegal activities including CSAM,[25] San Francisco's (U.S.) lawsuit against websites that create deepfake AI-facilitated NCII,[26] lawsuits against X by the governments of Baltimore

(U.S.),[27] the Netherlands' action against the mass facilitation and spreading of AI-facilitated NCII by Grok,[28] and Meta being sued by the New Mexico (U.S.) government for enabling harm, including child sexual exploitation, against its users.[29]

EU agrees to ban nudification apps to protect citizens

The European Union has recently reached a political agreement to simplify implementation of the *AI Act* (the comprehensive European regulation on AI) while strengthening protections against harmful AI-generated sexual content. The agreement prohibits AI systems designed to generate NCII (including nudification apps), as well as AI-generated CSAM. EU institutions have framed the changes as an effort to balance innovation, competitiveness and fundamental rights protections.[30]

GENERAL OVERVIEW OF REGULATORY FRAMEWORKS AND PUBLIC POLICY WORLDWIDE

AI-facilitated NCII non-consensual intimate imagery builds on a form of harm that has been addressed in policy and legal frameworks for over a decade. However, its initial framing as "revenge porn" narrowed the issue, obscured its structural and gendered dimensions, and left gaps around synthetic content and platform accountability.

Below is a brief analysis of global regulatory trends concerning NCII and CSAM, alongside an overview of the current legal framework in the U.S., highlighted given that country's central role as the primary jurisdiction for most platform governance.

Common trends in the regulation of non-consensual intimate images

Only 58 of 190 countries have enacted legislation to protect women against cyber harassment, protecting less than half of the population, and only 7 economies provide either damages and/or financial compensation for survivors, in addition to criminal penalties.[31] When it comes to digital NCII, as of 2025, 117 countries reported efforts to address them.[32] The following table presents selected legislation from around the world addressing AI-facilitated NCII:

Legislation around the world to address AI-facilitated NCII

Country	Legal instrument	Year	Scope of criminalization	Penalties	Notable features
Australia	*Criminal Code* Amendment (Deepfake Sexual Material) Bill[33]	2024	Creation and distribution of NCII (incl. AI-generated).	Up to 7 years' imprisonment.	• Emphasis on legal clarity and harmonization. • The Law Council cautioned against overreach; the Senate supported the bill with review and harmonization recommendations. • First prosecution under the new federal offence in 2026.[34]
Canada	Protecting Victims Act (Bill C-16, Legislation to protect victims and keep kids safe from predators)[35]	2026	To explicitly cover non-consensual deepfakes, the Protecting Victims Act prohibits the NCII distribution, and makes illegal the threat to distribute NCII, including deepfakes. The *Criminal Code* already made illegal to distribute intimate images without consent, but did not cover threats to release such images, which are a feature of many sextortion cases. Creation of new offences to cover deepfakes used as CSAM, and depiction of bestiality.	Up to 10 years' imprisonment.	• Increase from 5 to 10 years of imprisonment the maximum penalty when the offence is prosecuted by indictment for the threat to distribute intimate images, including sexual deepfakes, without the consent of the person depicted. • Inclusion of an aggravating factor to the offence of extorsion when it is committed in the context of sextortion cases. • Restoration of all mandatory minimum penalties (MMPs) that had been inoperative following findings of unconstitutionality by the Supreme Court of Canada, except where the MMP would result in grossly disproportionate punishment.
Denmark	*Danish Copyright Act*[36]	2025	Unauthorized use of likeness including image and voice, as protected under copyright law.	Platform fines; removal obligations.	• Two-tier protection: General safeguards against realistic digital likeness and specific rights for performers. • Regulates the image and voice, and is being used for topics around deepnudes. • Enforced via the EU Digital Services Act. • Effective July 2026.

Legislation around the world to address AI-facilitated NCII (continued)

Country	Legal instrument	Year	Scope of criminalization	Penalties	Notable features
South Korea	*Act on Special Cases with Respect to Punishing Sex Crimes*[37]	2024	Creation, distribution, possession and viewing of NCII (incl. AI-generated).	Up to 7 years (production or distribution); up to 3 years or fines (possession or viewing).	• Triggered by the proliferation of deepfake sexual content in a Telegram chat with 22,000+ members.[38] • Broad prohibition including consumption.
United Kingdom	*Data (Use and Access) Act* (DUAA)[39]	2025	Creation and solicitation of NCII (incl. AI-generated).	Up to 6 months + unlimited fines.	• Builds on earlier gaps (2015 "revenge porn" law, *2023 Online Safety Act*). • Driven by advocacy efforts.

Despite recent regulatory advances in some countries, such as in Canada, the broader regulatory architecture often remains structurally incomplete. Six structural cross-jurisdictional gaps stand out in normative frameworks around technology-facilitated gender-based violence (TFGBV): 1) fragmented and inconsistent definitions; 2) a predominance of non-binding commitments over enforceable obligations; 3) uneven regional progress; 4) delays between adoption and implementation; 5) limited platform and AI accountability; and 6) persistent data and monitoring gaps.[40]

The above trends shape legislation in three key ways: 1) many countries continue to rely on narrow, offence-specific provisions rather than integrated legal frameworks; 2) cybercrime and online safety laws frequently lack a gendered perspective; and 3) enforcement is weak due to limited institutional capacity and a lack of binding obligations for technology companies.

Common trends in the regulation of child sexual abuse material

The regulatory landscape for CSAM has evolved significantly in recent years, yet critical gaps remain, particularly around digitally generated content. A 2023 review[41] assessed national legislation across 196 countries against five criteria: 1) criminalization of CSAM; 2) legal definition; 3) criminalization of technology-facilitated offences; 4) prohibition of possession regardless of intent to distribute; and 5) mandatory reporting for internet service providers. The study showed that only 32% of countries had any legislation, and of those, 40% did not address technology-based offences. Only 27 of 196 met all five criteria, among them Canada. Mexico met four, falling short on mandatory reporting obligations for internet service providers.

The gap is even wider for digitally generated CSAM. A 2024 study[42] covering 49 countries found that nine of them do not explicitly criminalize this AI- or digitally child-harmful synthetic content. In five of them, its treatment is context-dependent, and in four others (including Mexico) legality hinges on whether a real child is depicted, leaving synthetic content with no identifiable survivor outside the law.

A survey among individuals who had searched for CSAM on the so-called dark web found that nearly three in ten reported having viewed such AI-facilitated abusive content to minors, while one in ten admitted to having created it themselves with minimal effort.[43]

United States: The *TAKE IT DOWN Act* and beyond

Regulation of NCII and CSAM in the U.S. is particularly relevant for Canada and Mexico. Their digital ecosystems are deeply intertwined with U.S.-based platforms and their regulatory approaches are shaped by commitments under the Digital Trade Chapter[44] of the Canada–United States–Mexico Agreement (CUSMA).

Before 2025, survivors in the U.S. faced a fragmented patchwork of state laws, limited federal recourse, and platform immunity for third-party content under Section 230.[45] This shifted in 2025–2026 with the enacting of two landmark bipartisan laws. Table 2 shows the new U.S. laws addressing AI-facilitated NCII.

U.S. legislation to address AI-facilitated NCII

Instrument	Year enacted	Focus	Key provisions
TAKE IT DOWN Act[46] (Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks)	2025	Criminal	• Criminalizes intentional publication of NCII (incl. AI-generated). • 48-hour platform removal obligation. • Financial penalties and up to 2 years' imprisonment. • Enhanced penalties for cases involving minors.
DEFIANCE Act[47] (Disrupt Explicit Forged Images And Non-Consensual Edits)	2026	Civil	• Expands survivor options beyond criminal justice. • Enables civil litigation for financial and emotional damages.[48]

Implementation, however, raises unresolved challenges. The effective removal of content depends on robust identity verification to prevent fraud, while the 48-hour deadline (viewed as insufficient) strains platforms without offering funding or compliance guarantees. Additionally, the extraterritorial reach of both laws hinges on the cooperation of global actors amid rising geopolitical tensions and fragmentation.[49]

Regarding the protection of minors, the Senate unanimously passed the *STOP CSAM Act* of 2025,[50] which expands platform liability by introducing a recklessness standard. This means platforms can be held liable for hosting or facilitating CSAM, even without explicit knowledge. The law targets the active promotion and passive storage of such material, including AI-facilitated material, closing a gap that previously allowed platforms to avoid

accountability by claiming ignorance. Critics warn, however, that these new provisions could be used by companies to justify weakening or abandoning end-to-end encryption, with broader implications for user privacy and secure communications.[51]

Alongside these legislative developments, the National Center for Missing & Exploited Children (NCMEC) has introduced two complementary tools: the *Take it Down*[52] service, allowing minors to request the removal of intimate content without police involvement or formal legal proceedings; and the CyberTipline,[53] a centralized national reporting system for online child sexual exploitation covering grooming, trafficking, CSAM and AI-facilitated content. There are limitations, however, including the fact that only image and video formats are covered, leaving out audio and/or text files.[54]

COUNTRY PROFILE: CANADA

This section examines the landscape of NCII, including CSAM, in Canada. It outlines the current regulatory and complaint mechanisms, and identifies the key gaps in addressing both the creation and distribution of AI-facilitated NCII.

Overview of non-consensual intimate images abuse in Canada

In 2022, police recorded 896 reported cases of NCII distribution.[55] Broader estimates, however, suggest approximately 275,000 survivors and 2.37 million NCII images annually.[56]

Despite this evidence, significant data gaps remain. Disaggregated data on AI-facilitated NCII (broken down by specific demographic variables, such as gender, sex, place of residence, ethnicity, and other relevant characteristics) are largely unavailable, making it difficult to assess how the phenomenon is evolving alongside the rapid adoption of Generative AI. While Canada has not experienced a high-profile trigger case, the problem is well documented and growing, with clear impacts on young women's dignity, privacy, health and participation in public life.

The following boxes highlight selected public cases of AI-facilitated NCII in the country.

AI-facilitated NCII cases in Canada

→ **Quebec man sentenced for AI-generated child pornography (2023)**[57]

A man was sentenced to an eight-year term for using AI to create CSAM videos. He pleaded guilty to producing at least seven deepfake videos and possessing more than 545,000 CSAM files. While the defense argued for a lighter sentence on the basis that no physical abuse occurred, the judge held that the creation of such material constituted a renewed violation of the survivors' sexual integrity.

→ **AI-facilitated nude photos of girls from Winnipeg school posted online (2023)**[58]

In 2023, it was discovered that AI-generated NCII involving underage students at a local school in Winnipeg were being circulated online. The school alerted families, contacted police and activated survivor support protocols, while also engaging Cybertip.ca and Project Arachnid to report and remove the content.[59] No charges were filed, with police pointing to evidentiary challenges, survivors' willingness to proceed, low likelihood of conviction and legal complexities related to AI-generated content.[60]

→ **Fake nudes posted by London Catholic students (2024)**[61]

The students of a local secondary school shared AI-facilitated NCII of their female classmates in group chats. The police launched an investigation, and the school warned of possible disciplinary action. Months later, however, no criminal charges had been filed against the students involved. The London District Catholic School Board did not disclose whether any disciplinary measures were taken, and it refused to answer journalists' questions.[62]

Regulatory framework

The Protecting Victims Act (Bill C-16) came into force on June 18, 2026. The Act amends the *Criminal Code* and other legislation to respond to modern threats and strengthen protections for victims. According to Canada's Department of Justice, these reforms represent "one of the most consequential updates in generations to address delays, protect victims and survivors of gender-based violence, including sexual violence and intimate partner violence, and to keep our kids safe from predators".[63]

The Act touches on several criminal and correctional statutes, including provisions related to the AI-generated NCII distribution. Specifically, it broadens the offence of NCII distribution to include visual representations created by mechanical or electronic means (deepfakes). The *Criminal Code*'s definition of "intimate image" now covers AI-facilitated synthetic content, making the offence easier to enforce. The Act also reinstates mandatory minimum penalties for several offences, including the distribution of NCII and voyeurism, and creates new offences, notably threatening to distribute CSAM, including deepfakes, and threatening to distribute NCII, including sexual deepfakes.[64]

In the coming months, it will be critical to assess the effectiveness of these new measures and the resources allocated to their implementation, including training provided to legal professionals, police forces, and support workers.

This new law targets individual offenders, unlike Bill C-63 (the Online Harms Act), which focused instead on imposing regulatory obligations on platforms. C-63 died on the Order Paper in 2025 when Parliament was dissolved ahead of the last federal election. Bill C-34, introduced in June 2026, revives this regulatory approach to address digital harms more effectively.[65]

Awaiting new regulatory obligations for platforms

In June 2026, the Government of Canada introduced Bill C-34 (Safe Social Media Act), which seeks to expand obligations for digital platforms to address harmful content, including deepfakes.

The Safe Social Media Act would enact two new Acts: The Digital Safety Act and the Digital Safety Commission of Canada Act. Its scope would extend beyond social media platforms to include AI-powered chatbots services and other digital services, websites and applications. However, as of the date of this report, the bill remains at an early stage of the legislative process (first reading stage), and its provisions may still undergo significant changes. Several grey areas remain to be clarified.[66]

Privacy protection

Additionally, the Office of the Privacy Commissioner offers a route grounded in data protection rather than criminal law. Where personal data or likeness is used without consent to generate synthetic sexual content, the Commissioner can investigate organizational compliance, placing obligations on the entities involved in content creation and distribution, not only on individual perpetrators.[67] This framing gained relevance after the Commissioner launched an investigation into xAI and X over the use of its tool Grok to generate NCII in early 2026.[68]

Provincial frameworks

Provincial frameworks, in turn, vary significantly in their capacity to address AI-facilitated NCII. Québec's *Loi visant à contrer le partage sans consentement d'images intimes*[69] *(Act to counter non-consensual sharing of intimate images)*, that came into force in June 2025, explicitly defines an intimate image as "any image, altered or not, that represents or appears to represent a person either nude [. . .] or engaging in an explicit sexual activity." This formulation extends coverage to digitally

altered and potentially synthetic content, similar to what has been adopted in similar frameworks by other provinces. This includes British Columbia's *Intimate Images Protection Act*,[70] which enables survivors to seek both content removal and civil compensation, supported by an institutional accompaniment service, as well as New Brunswick (*Intimate Images Unlawful Distribution Act*, SNB 2022)[71] and Prince Edward Island (*Intimate Images Protection Act*, RSPEI 1988).[72] In contrast, the language in the frameworks of Alberta and Nova Scotia is too narrow to clearly cover AI-altered or generated content, despite the latter province operating Cyberscan,[73] a dedicated resource centre for intimate image abuse. Ontario has no provincial framework in place.

Regarding minors, Ontario and Québec require post-secondary institutions to have sexual violence response policies, while most other provinces leave this to institutional discretion. Although these measures offer avenues for content removal and compensation, they largely fail to address survivors' long-term psychological harm and the broader structural dimensions.[74]

Canada's federal structure adds a further layer of complexity. Criminal law is a federal matter, but law enforcement is predominantly a provincial responsibility with no supremacy clause.[75] Provincial civil regulatory frameworks, which offer varying levels of protection from one province to another, coexist with federal criminal law, but this multi-layered system can be complex. As a result, the most protective civil frameworks are concentrated in a handful of provinces, and a survivor's access to justice depends significantly on geography.

Complaint and redress mechanisms

Canada's redress landscape offers meaningful but geographically uneven pathways for survivors. The strongest mechanisms exist at the provincial level, with federal oversight playing a complementary but limited role.

Québec's "ordonnance de cessation ou de prévention"[76] (cease-and-prevent order) stands out as the country's most structured urgent-response mechanism. It enables expedited, summary applications supported by official forms, reducing procedural barriers for survivors without legal representation, and allowing for exceptional measures when urgency demands immediate intervention. British Columbia's *Intimate Images Protection Act* also offers institutional support that guides survivors through the process, in addition to emotional support and referrals.[77]

For cases involving minors, Cybertip.ca,[78] Canada's national tipline for reporting the online sexual exploitation of children, operated by the Canadian Centre for Child Protection, provides a dedicated reporting channel covering offences such as CSAM, online luring, sextortion and AI-facilitated NCII (explicitly). The platform also operates Project Arachnid, a technology tool that issues thousands of content removal notices per month to platforms hosting CSAM.

Regulatory, implementation and coordination gaps

Canada's response to AI-facilitated NCII remains constrained by a set of structural limitations that undermine its effectiveness in practice:

→ **Outdated regulatory privacy frameworks**

Canada's privacy regime, largely designed in a pre-generative AI context, is increasingly ill suited to address the challenges posed by synthetic content. This limitation is especially acute for children and adolescents, whose exposure to AI-facilitated CSAM falls outside what existing frameworks were designed to manage.[79]

Moreover, existing privacy laws lack meaningful enforcement mechanisms, including criminal penalties and administrative monetary sanctions. As a result, the current framework operates more as a set of voluntary standards than as a binding regulatory regime, despite the existence of proposed reforms that have yet to be enacted.

→ **Institutional fragmentation and capacity constraints**

Canada's response is weakened by fragmentation across legal and institutional frameworks. Criminal enforcement, civil remedies and privacy protections operate across largely disconnected regimes (*Criminal Code*, provincial civil systems and data protection oversight), without an overarching mechanism to ensure coherence. As a result, survivors' access to remedies and levels of protection vary significantly by jurisdiction and legal pathway.[80]

Institutional capacity is another constraint. In Canada, decisions to pursue criminal charges rest with Crown prosecutors rather than the police, creating an additional institutional filter and leading to a disconnect between investigation and charging. Additionally, cases often hinge on explaining complex technologies to courts with limited technical expertise, while officers receive limited training in areas like digital forensics and platform-specific abuse. These challenges are compounded by resource constraints, unclear documentation protocols and uncertainty around legal thresholds for digital evidence.[81]

→ **Perpetrator identification and cross-jurisdictional cases**

Identifying perpetrators remains one of the most significant operational barriers. While cases involving traditional types of NCII may be traceable, attribution is often difficult in AI-facilitated cases, rendering prosecution unfeasible. This challenge is particularly acute in cross-jurisdiction cases, where domestic enforcement has limited reach.

→ **Gaps in prevention and institutional responses**

Preventive and educational responses also remain uneven. While some provincial curricula include components on sexual violence and digital harms, their implementation is inconsistent and often dependent on individual educators and local policies. At the post-secondary level, dedicated sexual violence prevention frameworks have been diluted since 2021, frequently absorbed into broader equity, diversity and inclusion (EDI) initiatives.

→ **Inequalities in access to justice**

Access to justice is another barrier. Individuals with greater financial resources, social capital or familiarity with legal systems re better positioned to seek redress and navigate available mechanisms. In contrast, First Nation and racialized communities face additional systemic barriers, including historical mistrust of law enforcement and the justice system, significantly reducing reporting rates and access to support.

Country profile: Mexico

This section examines the landscape of NCII, including CSAM, in Mexico. It outlines the current regulatory and complaint mechanisms, and identifies the key gaps in addressing both the creation and distribution of AI-facilitated NCII.

Overview of non-consensual intimate images abuse in Mexico

The most recent estimates indicate that 84.46% of survivors are women, with those aged 21–35 accounting for nearly a third of cases.[82] Moreover, 43.2% of women and girls who experienced cyberbullying reported being threatened with the publication of personal data or intimate material as a form of extortion, with cisgender men implicated in 80% of incidents and identified as the primary aggressors in 70%.[83]

Exposure to online abuse also begins early. Young women aged 18–24 are 27% more likely to experience online violence than their male peers.[84] Most girls report their first experience of online harassment between the ages of 14–16, with nearly half receiving threats of physical or sexual violence.[85]

The scale of harm is further amplified by high levels of consumption, with Mexico ranking among the top five countries globally in traffic to the most-visited NCII-hosting websites.[86] The impact is particularly severe for minors, as Mexico ranks among the

countries with the highest global rates of CSAM production and distribution, with the northern city of Juárez alone accounting for 60% of identified CSAM files worldwide.[87] Moreover, reported cases increased by 86% in the first half of 2025, with girls representing 59% of those affected.[88]

The following boxes highlight the two most famous AI-facilitated NCII cases in the country.

AI-facilitated NCII cases in Mexico

→ **The IPN Case (2023)**[89]
A large-scale case of AI-facilitated NCII emerged at the Instituto Politécnico Nacional (IPN), where authorities uncovered 166,000 synthetic files, including 20,000 videos, with at least 40% involving female students aged 17–25. A student was initially arrested for digital sexual violence, but part of the conviction was later overturned due to insufficient evidence. After authorities confirmed that some material involved minors, charges for possession and distribution of CSAM led to a five-year prison sentence and a fine. The case remains partially unresolved, with appeals ongoing and survivors reporting institutional neglect and revictimization.

→ **The Zacatecas case (2025)**[90]
At least 400 female students from a secondary technical school in the Mexican state of Zacatecas reported the creation and circulation of AI-facilitated NCII. Investigations suggest that three male teenagers from the same institution created and disseminated the content, but at the time of this report, no sentence had been handed down.

Regulatory framework

Mexico has one of the most extensive legal frameworks globally for addressing digital violence. A central pillar is the *Ley Olimpia*[91] (Olimpia Law), a set of legislative reforms initiated in 2018 that established digital violence as a legally recognized category and criminalized violations of sexual privacy through digital means, including NCII distribution. While these reforms extend beyond authentic images to include altered content, allowing AI-facilitated NCII to fall within existing definitions, their application to synthetic content remains uneven in practice.

First adopted in the state of Puebla in 2018, the Olympia Law has since been implemented across all 32 Mexican states through amendments to state criminal codes, criminalizing NCII nationwide. However, this expansion has relied on varying legal definitions and terminology, leading to inconsistencies in how offenses are defined, investigated, and prosecuted.[92]

The federal framework was further strengthened in 2021 through amendments to the *Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*[93] (General Law on Women's Access to a Life Free of Violence) and to the *Código Penal Federal* (Federal *Criminal Code*).[94] These reforms formally incorporated digital violence into the national legal framework and expanded tools for prevention and redress, but do not explicitly cover AI-facilitated NCII.

In cases that intersect with exploitation, the *Ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos*[95] (General Law to Prevent, Punish and Eradicate Crimes Related to Trafficking in Persons and for the Protection and Assistance to Victims of these Crimes) establishes restrictions on non-consensual pornography, particularly where it involves sexual exploitation, minors or individuals with disabilities, or where third parties profit from the content. These provisions can be applied in certain NCII cases, often carrying higher penalties and benefiting from stronger institutional mechanisms than do standard digital violence provisions.[96]

Finally, despite recent regulatory developments, protections for children against digital violence remain limited. The Federal *Criminal Code*[97] defines child pornography as any act involving the trafficking, distribution or display of minors through writings, recordings, photographs or images, whether real or simulated, by a person who uses any means or method. Similarly, anyone who stores, purchases or rents such material without intending to sell or distribute it is subject to imprisonment for one to five years, plus fines.[98]

Complaint and redress mechanisms

At the judicial level, the Supreme Court of Justice of the Nation has developed a protocol for adjudicating cases from a gender perspective.[99] It guides how courts examine context, assess facts and evidence, identify intersecting forms of discrimination, recognize gender stereotypes and biases, and determine reparations.[100] In civil matters, Article 1916 of the Federal Civil Code[101] enables moral damages, a remedy available to survivors of NCII dissemination who seek an alternative to criminal proceedings.

At the institutional level, Mexico City is the only jurisdiction with a specialized agency for digital sexual crimes,[102] but it faces a number of challenges. It not only relies on external support for technical investigations, but its staff is primarily trained in human trafficking, reflecting a lack of specialized digital expertise. The Línea Mujeres[103] telephone service provides guidance and support for women experiencing violence, but when cases involve digital violence, they are transferred to the National Guard's Cyber Police, which is not specialized in gender matters.

The protection of minors, in turn, is coordinated by the National System for the Protection of Children and Adolescents,[104] but it was not designed to address AI-facilitated NCII specifically.

Many of the gaps left by institutional mechanisms are filled by civil society. Organizations including Cultivando Género,[105] Defensoras Digitales,[106] Hijas de Internet,[107] Luchadoras[108] and SocialTic,[109] among others, provide digital safety education, prevention resources and direct support to survivors where formal institutions are absent, inadequate or inaccessible.

October 2026 Regulatory Update: New obligations for digital platforms

Mexico adopted a decree establishing new obligations for digital platforms to protect minors from harmful online content, including age verification and content removal measures.

Although mandatory, the decree does not provide sufficiently detailed technical guidelines for implementation and oversight, nor does it establish specific penalties for noncompliance. The government has described it as non-punitive, indicating that legislation introducing penalties could follow if platforms fail to comply.

While the decree does not explicitly address NCII, some provisions may apply when minors are involved. The decree illustrates the ongoing challenge of translating regulatory obligations into effective platform accountability.

Source: *Presidencia de la República (2026, October 14), Presidenta Claudia Sheinbaum firma decreto de entornos digitales seguros para niñas, niños y adolescentes.*

Regulatory, implementation and coordination gaps

Despite the mechanisms described above, Mexico's response to AI-facilitated NCII is constrained by a set of structural limitations that reveal a profound disconnect between the breadth of the legal framework and the institutional capacity to operationalize it.

→ **Implementation over legislation**

The core problem in Mexico is not a lack of norms, but the limited institutional capacity to implement them. Prosecutors often lack clarity on what evidence to request, how to incorporate these offenses into an investigation or how to build cases that withstand judicial scrutiny. Many prosecutors' offices avoid NCII cases altogether, fearing that judges will demand evidentiary standards equivalent to those required in human trafficking cases, standards that are not only disproportionate to the penalties involved, but also often ill-suited to AI-facilitated NCII, where traditional forms of evidence may not exist.

A further complication lies in the terminology itself. The offence is defined under different names, allowing prosecutors to interpret and classify conduct based on their own criteria. This interpretive variability introduces inconsistency at the very first point of institutional contact and can determine whether a case proceeds at all. Of 1,500 complaints filed in 2021 for NCII distribution, only 8 reached the judiciary, representing 0.5% of cases.[110] Instead, many reached conditional agreements or summary judgments, but the number of these remains unknown.

→ **Institutional capacity and judicial gaps**

Public authorities often lack gender-sensitive and technical training, limiting their ability to respond effectively to digital abuse. This is reflected in the shortage of specialized personnel, as well as the absence of clear, standardized protocols.[111] In practice, these gaps can discourage reporting, particularly when survivors anticipate revictimization, further compounded by the persistent minimization of digital harms as "not real" when content is synthetic.

→ **Burden of proof on survivors**

Survivors are often required to prove their credibility, collect and preserve their own evidence, and navigate complex digital evidentiary processes, handling screenshots, metadata, URL preservation, platform procedures and cross-jurisdictional inconsistencies.[112] Unlike cases involving physical harm, the psychological, financial, social and professional damage caused by NCII is difficult to quantify through standard evidentiary tools.

→ **The protection gap for minors**

The Mexican *Ley general de educación*[113] (General Education Law) requires schools to have violence prevention and response protocols, but these have not been adapted to address image-based abuse, digital violence or AI-facilitated content. Schools have developed campaigns against traditional bullying, but have not translated them to the digital sphere either.

→ **Data and evidence gaps**

Mexico's data landscape is insufficient for evidence-based policymaking. The National Institute for Statistics and Geography's (INEGI) cybersecurity data lacks the detail needed to combat AI-facilitated NCII. There are no reliable metrics distinguishing synthetic from real content, no end-to-end tracking of cases from report to resolution, and no comprehensive public data on perpetrator profiles (e.g., age, gender and relationship to survivors).

KEY COMPARATIVE FINDINGS

Canada's and Mexico's responses to AI-facilitated NCII reveal a paradox that runs through both countries. Despite operating from very different legal traditions, institutional architectures and resource contexts, both arrive at similar outcomes for survivors, as shown in the table below.

Comparative findings in Canada's and Mexico's responses to AI-facilitated NCII

	Mexico	**Canada**	**Commonality**
Legal coverage of synthetic content	*Ley Olimpia* covers modified/altered content in principle; inconsistent application across 32 jurisdictions.	The Protecting Victims Act (Bill C-16, passed) expands the *Criminal Code* definition of NCII to include AI-facilitated synthetic content, including sexual deepfakes. It also criminalizes treats to distribute intimate images, including sexual deepfakes.	• Both countries have moved toward recognizing AI-enabled harms within existing NCII frameworks. However, regulation remains primarily focused on individual offenses and harmful outcomes rather than the broader AI generation and dissemination ecosystem.
Platform accountability and prevention	Limited platform-specific obligations and reliance primarily on criminal and civil remedies.	Individual liability has been strengthened through the Protecting Victims Act (Bill C-16, passed), while broader platform obligations remain under development through Bill C-34 (Social Media Act), which is still under legislative review.	Neither country currently has a fully developed framework addressing the role of platforms in preventing, detecting, and responding to AI-generated NCII at scale.

Comparative findings in Canada's and Mexico's responses to AI-facilitated NCII (continued)

	Mexico	Canada	Commonality
Institutional capacity	Near-absent outside Mexico City's agency dedicated to digital sexual crimes; no specialized infrastructure in most of the country.	Fragmented across federal/ provincial lines; uneven Crown attorney capacity and judicial tech literacy.	Both face a justice system ill-equipped to handle the technical complexity of AI-facilitated NCII cases.
Redress mechanisms	Article 1916 of the Federal *Civil Code* as an alternative to pursue moral damages. Civil society fills critical gaps left by formal institutions.	Reporting and redress mechanisms are primarily concentrated at the provincial level. Quebec and British Columbia offer specific avenues for requesting the removal or cessation of the distribution of intimate images. For minors, Cybertip.ca provides a specialized national channel for reporting and content removal.	Survivor-centred redress depends on geography and available resources, not on a coherent national framework.
Protection of minors	Stronger framework under human trafficking law; minor perpetrators rarely prosecuted; schools unprepared.	CSAM provisions cover AI-facilitated content; juvenile system flexible; educational responses inconsistent.	Both have stronger legal frameworks for CSAM than for adult NCII, yet schools in both countries have failed to adapt violence prevention protocols to digital environments.
Data and evidence	Insufficient disaggregated data on synthetic content.	Aggregate NCII data exists; AI-specific metrics largely unavailable; no standardized reporting categories.	Neither country can fully measure the scope of AI-facilitated NCII; policymakers are designing responses to a problem without sufficient data.
Access to justice for survivors	Burden on survivors; revictimization common; only 0.5% of complaints reach the judiciary.	Legal aid costly; burden of proof on survivors; shame suppresses reporting; vulnerable groups face compounding barriers.	In both countries, survivors bear a disproportionate burden; the most marginalized (Canadian First Nations, Mexican Indigenous, racialized communities, minors) face the greatest barriers to justice.

The lack of platform accountability: a problem in both countries

Among the convergences identified in this comparative analysis, none is more consequential than the limited capacity of both countries to hold digital platforms accountable. Because most platforms where AI-facilitated NCII is created, distributed and monetized are U.S.-based, Canada and Mexico face a similar structural constraint in regulating them.

This challenge is reinforced by the CUSMA's Digital Trade chapter, which restricts governments' ability to impose requirements (such as algorithmic transparency, data localization or local presence) to platforms, weakening digital sovereignty and access to justice. In practice, platforms frequently decline to provide information needed to identify perpetrators, citing privacy obligations. Even when content is removed, it frequently reappears, and platforms face few consequences or incentives to improve detection and enforcement.

These challenges are further compounded by the transjurisdictional nature of the harm. When perpetrators operate across borders, legal recourse becomes far more complex. Although complaints can be filed, extradition is rarely viable, as NCII-related offenses are often classified as minor crimes in international cooperation frameworks. As a result, many cases remain effectively beyond the reach of enforcement, regardless of the strength of domestic legislation.

PUBLIC POLICY RECOMMENDATIONS

Both Canada and Mexico face structural constraints that no domestic framework can resolve in isolation: U.S.-based platforms operating beyond their regulatory reach, definitional inconsistencies that complicate cross-border cooperation, and a protection gap for minors that requires coordinated educational responses. The following recommendations address these shared challenges through multilateral and bilateral mechanisms.

Cross-cutting policy recommendations

Standardize definitions of AI-facilitated non-consensual intimate images

→ Leverage multilateral mechanisms to prioritize 1) an international definition of TFGBV and DGBV inclusive of AI-facilitated NCII and 2) cross border cooperation for legal responses around NCII, including the Organization of American States (OAS), specifically the Inter-American Commission of Women (CIM), the UN Women Beijing+30 process and the OECD's AI governance frameworks, among others.

Leverage the Canada–United States–Mexico Agreement for platform accountability

→ Advance a coordinated position on platform accountability in the upcoming CUSMA review, drawing on the documented failures of the current Digital Trade chapter.

→ Explore existing binding models, including the EU *Digital Services Act*'s risk assessment obligations and the *TAKE IT DOWN Act's* 48-hour removal requirement, as precedents for what enforceable platform standards could look like in practice.

→ Pursue an agreement to establish minimum platform cooperation standards for all NCII

cases, including mandatory response timelines for law enforcement information requests and obligations to prevent recirculation of reported content.

- → Require platforms to implement proactive detection of known CSAM using existing hash-matching technologies as a baseline obligation in both jurisdictions.

Develop a bilateral cooperation mechanism for cross-border non-consensual intimate images cases

- → Establish structured mechanisms for cross-country knowledge exchange among civil society organizations, legal practitioners and institutional actors; including study visits, joint training programs and shared documentation of effective practices.
- → Formalize said exchanges via bilateral agreements between organizations, joint funding mechanisms or a standing Canada-Mexico working group on NCII, plus links between both countries' prosecutors' offices and the Canadian Centre for Child Protection.
- → Develop bilateral research projects to further document the challenges around AI-facilitated NCII, fostering intersectional and gender-based research.

Address the protection gap for minors through education

- → Integrate digital literacy and online safety as core curriculum components across all levels, including topics such as consent, synthetic content, digital manipulation, privacy and cyber harassment dynamics, informing students of their rights, reporting mechanisms, consequences and available support services.
- → Mandate the adaptation of school violence prevention protocols to explicitly cover image-based abuse, digital violence and AI-facilitated content, ensuring that the legal obligation schools already have extends to the digital environment.
- → Design standardized guidance and practical tools for schools; for instance, an implementation-oriented manual that translates policy into protocols and procedures for the classroom.
- → Implement continuous, gender-sensitive training for educators, administrators and students. Particularly engage boys and young men in prevention efforts to challenge harmful norms and reduce perpetration.

Specific recommendations for Canada

Canada's legal framework contains the foundational elements needed to address AI-facilitated NCII, but two structural gaps undermine its effectiveness: fragmented institutional capacity across provinces, and survivor redress mechanisms that vary significantly by geography. The following recommendations prioritize closing these gaps.

Strengthen legal framework

- → Swiftly implement the measures and policies needed to maximize the effectiveness of the Protecting Victims Act (Bill C-16), particularly by ensuring adequate training for legal professionals, police forces, and workers supporting victims.
- → Prioritize the adoption of Bill C-34 and ensure that any future federal online harms legislation introduces binding obligations for platforms. Such legislation should go beyond voluntary measures, including digital watermarking and algorithmic filters to detect synthetic intimate images, and establish clear enforcement mechanisms, including significant penalties for non-compliance.

Enhance institutional capacity to address AI-facilitated non-consensual intimate images

- → Develop a voluntary interprovincial training program for Crown attorneys, police and judges on the technical and evidentiary dimensions of AI-facilitated NCII cases, including digital forensics, platform evidence preservation and gender-sensitive adjudication.
- → Draw on existing frameworks in Québec and British Columbia as peer-developed models that

other provinces can adapt to their own legal and institutional contexts, facilitated through horizontal knowledge exchange rather than top-down implementation.

- → Create a dedicated federal coordination mechanism that connects provincial law enforcement, Crown prosecutors and civil society organizations working on NCII cases.

Strengthen and nationalize survivor-centred redress mechanisms

- → Extend Québec's cease-and-prevent order model, or an equivalent urgent content removal mechanism, to all provinces, establishing a national baseline for emergency redress that does not depend on geography.
- → Develop a national one-stop support pathway for NCII survivors, integrating legal guidance, content removal assistance, emotional support and referrals to local services, modeled on British Columbia's accompaniment approach.
- → Strengthen legal aid access for NCII cases affecting vulnerable populations, and explore dedicated funding streams for civil society organizations providing frontline legal accompaniment.
- → Establish a national survivor support initiative accessible to all ages, providing trained personnel, legal guidance, content removal support and emotional assistance via phone and chat. Canada's existing Cybertip.ca offers a strong foundation, but its mandate is limited to those under 18; expanding its scope could help fill this gap.

Specific recommendations for Mexico

Mexico's challenge is less a gap in legislation than a gap in implementation. The *Ley Olimpia* framework exists across all 32 states, but inconsistent definitions, limited specialized institutional capacity and a complaint process that places a disproportionate burden on survivors constrain its effectiveness. The following recommendations prioritize closing these gaps.

Prioritize the implementation of the existing legal framework over new legislation

- → Conduct a national audit of *Ley Olimpia*'s incorporation into state criminal codes, to identify where definitions are narrowest, enforcement is weakest and conviction rates are lowest, and use those findings to guide targeted federal intervention.
- → Develop binding national implementation protocols for NCII cases that standardize how prosecutors' offices classify, investigate and build cases under existing provisions. Establish clear prosecutorial guidelines that distinguish the standard of proof required for violations of sexual privacy from that required for human trafficking.
- → Establish technical criteria, oversight mechanisms, and penalties for digital platforms, particularly to prevent and address AI-facilitated NCIIs.

Build specialized institutional capacity at federal and state levels

- → Expand the specialized agency model currently operating in Mexico City, establishing minimum requirements, including on-site cyber police capacity, specialized personnel and gender-sensitive protocols.
- → Develop a national mandatory training program for prosecutors, investigators and judges on the technical dimensions of AI-facilitated NCII cases, including digital evidence preservation, chain of custody for online content, and the evidentiary tools available for cases where perpetrators operate anonymously or across jurisdictions.
- → Establish formal cooperation protocols between prosecutors' offices and civil society organizations, recognizing their technical expertise and survivor support as integral institutional assets.

Redesign the complaint process towards a survivor-centred approach

- → Establish a national one-stop digital violence reporting pathway that integrates complaint filing, evidence preservation guidance, legal

orientation, psychological support and content removal assistance in a single accessible mechanism, removing the current requirement that survivors navigate fragmented jurisdictions.

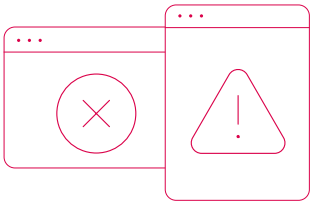
→ Eliminate institutional practices that function as barriers to reporting, including requirements that survivors produce evidence beyond their means, and demands for repeated testimony across multiple institutions.

→ Develop a national data collection system that tracks NCII complaints from initial report to resolution, disaggregated by type of content, jurisdiction and outcome, among others. Work with leading civil society groups to identify the type of data to be collected.

Conclusion

AI-facilitated NCII is no longer an emerging threat, but an entrenched and escalating form of technology-facilitated gender-based violence that disproportionately affects women, girls and children, with consequences that ripple across every dimension of their lives, including their safety, privacy, mental health, economic opportunities and ability to participate fully in public life. Across jurisdictions, technology continues to outpace policy, leaving survivors to navigate fragmented systems that were not designed to protect them.

The comparison between Canada and Mexico shows that, despite their different contexts, both countries face similar structural challenges with the limited leverage over the U.S.-based platforms, fragmented institutional responses and a persistent gap between legal recognition and effective implementation. The central challenge is not the absence of legislation, but the lack of specialized capacity, survivor-centred processes and coordinated governance needed to make existing protections work in practice. The evidence is clear. What remains is whether both countries will treat this issue with the urgency and seriousness it demands.



Notes

1. Security Hero (n.d.). *2023 State of deepfakes. Realities, Threats, and Impact.* https://www.securityhero.io/state-of-deepfakes/

2. Conger, K. et al., (2026, January 22). Musk's Chatbot Flooded X With Millions of Sexualized Images in Days, New Estimates Show. *The New York Times.* https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html

3. Vallance, C. (2026, January 8). Elon Musk's Grok AI appears to have made child sexual imagery, says charity. *BBC*. https://www.bbc.com/news/articles/cvg1mzlryxeo

4. Fry, D. (2025, October 10). Millions of children face sexual violence as AI deepfakes drive surge in new cases – latest global data. *The Conversation.* https://theconversation.com/millions-of-children-face-sexual-violence-as-ai-deepfakes-drive-surge-in-new-cases-latest-global-data-266171

5. UNICEF (2026). *'Deepfake abuse is abuse.'* https://www.unicef.org/lac/en/press-releases/deepfake-abuse-abuse

6. Wong, M. (2026, January 15). A Tipping Point in Online Child Abuse. *The Atlantic.* https://www.theatlantic.com/technology/2026/01/ais-child-porn-problem-getting-much-worse/685641/?mc_cid=d15749e2ca&mc_eid=3bc3a71315

7. Affoum, N., Santgostino, I., Vohra, N. & Wodon, Q. (2023). *Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws*. World Bank. https://documents1.worldbank.org/curated/en/099456506262310384/pdf/IDU0c7c3a5a70b56a04b250a31b0b32b8f5cd856.pdf

8. Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A. (2025). Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review. *Social Sciences & Humanities Open, 12*, 101882. https://doi.org/10.1016/j.ssaho.2025.101882

9. Kira, B. (2024, June 3). Deepfakes, the Weaponisation of AI Against Women and Possible Solutions. *Verfassungsblog*. https://verfassungsblog.de/deepfakes-ncid-ai-regulation/

10. Kopecký, K., & Voráč, D. (2026). The phenomenon of deep nudes—a new threat to children and adults. *AI & Society*, 41, 545–556. https://doi.org/10.1007/s00146-025-02425-4

11. Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., Sharkawy, A. (2025). Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review. *Social Sciences & Humanities Open, 12*, 101882. https://doi.org/10.1016/j.ssaho.2025.101882

12. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

13. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

14. Kristof, N. (2021, April 16). Why Do We Let Corporations Profit From Rape Videos? *The New York Times.* https://www.nytimes.com/2021/04/16/opinion/sunday/companies-online-rape-videos.html?smid=tw-share

15. Tech Transparency Project (2026, January 27). *Nudify Apps Widely Available in Apple and Google App Stores*. https://www.techtransparencyproject.org/articles/nudify-apps-widely-available-in-apple-and-google-app-stores

16. Mantzarlis, A. & Lakatos, S. (2025, July 14). AI Nudifiers continue to reach millions and make millions. *Indicator*. https://indicator.media/p/ai-nudifiers-continue-to-reach-millions-and-make-millions

17. AI Security Institute (2026). *International AI Safety Report 2026.* https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

18. Department for Science, Innovation and Technology (2025). *New law to tackle AI child abuse images at source as reports more than double.* Government UK. https://www.gov.uk/government/news/new-law-to-tackle-ai-child-abuse-images-at-source-as-reports-more-than-double

19. D'Anastasio, C. (2025, September 15). AI is replacing online moderators, but it's bad at the job. *The Star.* https://www.thestar.com.my/tech/tech-news/2025/09/15/ai-is-replacing-online-moderators-but-it039s-bad-at-the-job#goog_rewarded

20. Priyam, P. (2026, March 11). *Why AI Content Moderation Keeps Getting It Wrong — And a Framework to Fix.* LinkedIn. https://www.linkedin.com/pulse/why-ai-content-moderation-keeps-getting-wrong-framework-prachi-priyam-yhwuc/

21. This information was provided by the experts interviewed for this report. See the acknowledgements section for more information of the individuals interviewed.

22. For additional information, see: http://stopncii.org

23. For additional information, see: https://takeitdown.ncmec.org/

24. Meta. (2025, June 12). *Taking Action Against 'Nudify' Apps.* https://about.fb.com/news/2025/06/taking-action-against-nudify-apps/

25. Swiss Info (2025, January 18). El fundador de Telegram reconoció la «gravedad» de los hechos que le imputa la justicia francesa. *SWI swissinfo.ch.* https://www.swissinfo.ch/spa/el-fundador-de-telegram-reconoci%C3%B3-la-%22gravedad%22-de-los-hechos-que-le-imputa-la-justicia-francesa/88743834

26. Chiu, D. (2025, June 2). *City Attorney shuts down 10 websites that create nonconsensual deepfake pornography.* City and County of San Francisco. https://www.sf.gov/news-city-attorney-shuts-down-10-websites-that-create-nonconsensual-deepfake-pornography

27. Robins-Early, N. (2026, March 24). Baltimore sues Elon Musk's AI company over Grok's fake nude images. *The Guardian*. https://www.theguardian.com/technology/2026/mar/24/elon-musk-grok-ai-lawsuit-baltimore

28. Haeck, P. (2026, March 26). Dutch court bans Grok from generating fake nudes, threatens €100K daily penalties. *Politico*. https://www.politico.eu/article/netherlands-grok-x-ban-generative-pictures-penalties/

29. McQue, K. (2026, March 24). Meta ordered to pay $375m after being found liable in child exploitation case. *The Guardian*. https://www.theguardian.com/technology/2026/mar/24/meta-new-mexico-jury

30. European Commission. (2026, May 6). The EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens. [Press release]. European Comission. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024.

31. Affoum, N., Santgostino, I., Vohra, N. & Wodon, Q. (2023). *Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws*. World Bank. https://documents1.worldbank.org/curated/en/099456506262310384/pdf/IDU0c7c3a5a70b56a04b250a31b0b32b8f5cd856.pdf

32. Carmo, A. (2025, November 25). AI and anonymity fuel surge in digital violence against women. *United Nations News.* https://news.un.org/en/story/2025/11/1166411

33. Griffiths, O. (2024). *Criminal Code* Amendment (Deepfake Sexual Material) Bill 2024. *Bills Digest No. 81, 2023-24.* Parliament of Australia. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2324a/24bd081

34. Schriever, J. (2026, February 26). Deepfakes back in the headlines after a federal law was used for the first time. *Australian Broadcasting Corporation.* https://www.abc.net.au/news/2026-02-27/rise-in-sexualised-deepfakes-new-laws-explainer/106390940

35. Canadian Government (2026, June 18). *Protecting Victims Act: Legislation to protect victims and keep kids safe from predators*. https://www.justice.gc.ca/eng/csj-sjc/pl/c16/index.htm

36. Karttunen, S. (2026). *The Danish approach to copyright and deepfakes: A model for the EU?* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf

37. Carter, H. (2025, September 17). South Korea's Act on Special Cases with Respect to Punishing Sex Crimes. *Facia*. https://facia.ai/knowledgebase/south-koreas-act-on-special-cases-with-respect-to-punishing-sex-crimes/

38. Barr, H. (2024, August 29). South Korea's Digital Sex Crime Deepfake Crisis. *Human Rights Watch.* https://www.hrw.org/news/2024/08/29/south-koreas-digital-sex-crime-deepfake-crisis

39. Information Commissioner's Office. (2025). *The Data Use and Access Act 2025 (DUAA) – what does it mean for organisations?* https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/

40. UN Women, & Sexual Violence Research Initiative. (2025). *Global trends to prevent and respond to technology-facilitated violence against women and girls: A compendium of emerging practices.* https://www.unwomen.org/sites/default/files/2025-12/global-trends-to-prevent-and-respond-to-technology-facilitated-violence-against-women-and-girls-en_1.pdf

41. International Centre for Missing & Exploited Children. (2023). *Child Sexual Abuse Material: Model Legislation & Global Review.* https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf

42. Kuo, V., & Raidma, G. (2024). *Global CSAM Legislative Overview.* INHOPE. https://inhope.org/media/pages/articles/global-csam-legislative-overview-2024/71acaa8826-1765986997/executive-summary-global-csam-legislative-overview-2024.pdf

43. Protect Children. (2026). *CSAM Perpetrator Research Report: Findings from a Survey of CSAM Perpetrators on Digital Platform Use and Design (Tell Me More About Tech)*. Ofcom. https://www.protectchildren.fi/en/post/tmat-csam-perpetrator-research-report

44. Leblond, P. (2022). *The USMCA and digital trade in North America.* The Brookings Institution. https://www.brookings.edu/articles/usmca-forward-building-a-more-competitive-inclusive-and-sustainable-north-american-economy-digital/

45. Vargas-Chaves, I. (2025). Take it Down Act: un análisis crítico de su rol contra la difusión no consentida de imágenes y deepfakes. *Revista Criminalidad, 67*(3), 39-55. https://doi.org/10.47741/17943108.729

46. United States Congress. (2025, May 19). *TAKE IT DOWN Act (S.146, 119th Congress).* https://www.congress.gov/bill/119th-congress/senate-bill/146/text

47. United States Congress. (2025, May 21). *DEFIANCE Act of 2025 (H.R. 3562, 119th Congress).* https://www.congress.gov/bill/119th-congress/house-bill/3562

48. Mithani, J. (2026, January 13). Senate moves to let victims of sexually explicit deepfakes sue for damages. *The 19th*. https://19thnews.org/2026/01/senate-defiance-act-nonconsensual-images-deepfakes/

49. Aguirre-Lanegra, A., & Ramos, F. (2025). Deepfakes sexuales y violencia algorítmica: hacia un marco normativo integral de protección de la dignidad digital. *Estudios En Derecho a La Información, 11*(21), e20198. https://doi.org/10.22201/iij.25940082e.2026.21.20198

50. United States Congress. (2025, June 26). *STOP CSAM Act of 2025 (S.1829, 119th Congress).* https://www.congress.gov/bill/119th-congress/senate-bill/1829/text

51. Bowman, T. (2025, June 13). The STOP CSAM Act Would Make Kids Less Safe. *Center for Democracy & Technology*. https://cdt.org/insights/the-stop-csam-act-would-make-kids-less-safe/

52. For additional information, see: https://takeitdown.ncmec.org/

53. For additional information, see: https://www.missingkids.org/gethelpnow/cybertipline

54. Avendaño, E., Contreras, A., Macías, G., Paéz, S., Rivera, K., Samperí, A., Soria, E., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

55. Defend Dignity. (2024). *Submission to the Standing Committee on Canadian Heritage. Study: Harms Caused to Children, Women, and Men by the Ease of Access to, and Online Viewing of, Illegal Sexually Explicit Material.* https://www.ourcommons.ca/Content/Committee/441/CHPC/Brief/BR13053693/br-external/DefendDignity-e.pdf

56. Mortimer, S., Phippen, A., & Wright, D. (2025, March 12). The Scale of Non-Consensual Intimate Image (NCII) Abuse: A Data-Driven Global Analysis. *South West Grid for Learning.* https://swgfl.org.uk/magazine/the-scale-of-non-consensual-intimate-image-ncii-abuse-a-data-driven-global-analysis/

57. Serebin, J. (2023, April 26). Québec man who created synthetic, AI-generated child pornography sentenced to prison. *CBC News.* https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808

58. Bernhardt, D. (2023, December 15). AI-generated fake nude photos of girls from Winnipeg school posted online. *CBC News.* https://www.cbc.ca/news/canada/manitoba/artificial-intelligence-nude-doctored-photos-students-high-school-winnipeg-1.7060569

59. For additional information, see: https://cybertip.ca/en/

60. Rosen, K. (2024, February 16). No charges laid over explicit, AI-generated photos of Winnipeg students. *CTV News*. https://www.ctvnews.ca/winnipeg/article/no-charges-laid-over-explicit-ai-generated-photos-of-winnipeg-students/

61. Dubinski, K. (2024, April 4). Kids call for more lessons on AI after fake nudes posted by London Catholic students. *CBC News.* https://www.cbc.ca/news/canada/london/london-ontario-st-thomas-aquinas-sta-deepfake-ai-nude-sexual-imagery-1.7163183

62. Dubinski, K. (2024, April 25). No charges against Catholic high school students who made and shared deep-fake nudes of classmates. *CBC News.* https://www.cbc.ca/news/canada/london/st-thomas-aquinas-nude-photos-artificial-intelligence-1.7183878

63. Government of Canada (2026, June 18). *Protecting Victims Act: Legislation to protect victims and keep kids safe from predators*. https://www.justice.gc.ca/eng/csj-sjc/pl/c16/index.html

64. Government of Canada (2026, June 18). *Protecting Victims Act: Legislation to protect victims and keep kids safe from predators.* https://www.justice.gc.ca/eng/csj-sjc/pl/c16/index.html

65. Government of Canada (2026, June 10). *Government of Canada introduces legislation to make social media services and AI chatbots safer for children*. https://www.canada.ca/en/canadian-heritage/news/2026/06/government-of-canada-introduces-legislation-to-make-social-media-services-and-ai-chatbots-safer-for-children.html

66. Government of Canada (2026, June 10). *Bill C-34, the Safe Social Media Act.* https://www.canada.ca/en/canadian-heritage/services/safe-social-media-act.html

67. Office of the Privacy Commissioner of Canada. (2026, January 15). *Privacy Commissioner of Canada expands investigation into social media platform X following reports of AI-generated sexualized deepfake images.* https://www.priv.gc.ca/en/opc-news/news-and-announcements/2026/nr-c_260115/

68. Djuric, M. (2026, January 15). Canada's privacy watchdog investigating Musk's xAI over sexualized deepfakes. *Politico*. https://www.politico.com/news/2026/01/15/canadas-privacy-watchdog-investigating-musks-xai-over-sexualized-deepfakes-00731587

69. Québec Government. (2024). *Act to counter non-consensual sharing of intimate images,* CQLR c. P-9.0002. https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-9.0002?langCont=en

70. Government of British Columbia. (2026). *Intimate Images Protection Act.* https://www2.gov.bc.ca/gov/content/safety/public-safety/intimate-images/intimate-images-consent

71. Legislative Assembly of New Brunswick. (2022). *Intimate Images Unlawful Distribution Act,* SNB 2022, c. 1. https://canlii.ca/t/563w7

72. Prince Edward Island Government. (2021). *Intimate Images Protection Act,* RSPEI 1988, c. I-9.1. https://canlii.ca/t/54w8w

73. For additional information, see: https://novascotia.ca/cyberscan/

74. Salamis, B. (2025). *Stolen Faces: Policy Options to Mitigate Harm from Non-Consensual AI-Generated Intimate Image Abuse in Canada.* Simon Fraser University. https://summit.sfu.ca/_flysystem/fedora/2025-06/etd23790.pdf

75. Lyon, J. (1976). The Central Fallacy of Canadian Constitutional Law. *McGill Law Journal,* 22(1). https://lawjournal.mcgill.ca/article/the-central-fallacy-of-canadian-constitutional-law/

76. Québec Government. (n.d.). Non consensual sharing of intimate image. https://www.quebec.ca/en/justice-and-civil-status/support-victims-crime/non-consensual-sharing-intimate-image

77. McKenzie, T. & Kerr, L. (2024). *Québec B.C.'s New Intimate Images Protection Act.* BarTalk. https://www.bartalk.org/article/the-law/b-c-s-new-intimate-images-protection-act

78. For additional information, see: https://cybertip.ca/en/

79. Irwin, J, Dharamshi, A., Zon, N. (2021). *Children's Privacy in the Age of Artificial Intelligence.* Canadian Standards Association. https://www.csagroup.org/article/research/childrens-privacy-in-the-age-of-artificial-intelligence/?srsltid=AfmBOorVdFE_TMOCF-f0bVKRyGJQNflySTj8bOYfgxzAD20IgTAHAgdK

80. Siekierski, B. (2019). Deep Fakes: What Can Be Done About Synthetic Audio and Video? *Research and Education. Publication No. 2019-11-E.* https://publications.gc.ca/collections/collection_2019/bdp-lop/eb/YM32-5-2019-11-eng.pdf

81. Salamis, B. (2025). *Stolen Faces: Policy Options to Mitigate Harm from Non-Consensual AI-Generated Intimate Image Abuse in Canada.* Simon Fraser University. https://summit.sfu.ca/_flysystem/fedora/2025-06/etd23790.pdf

82. Aguirre, I., Barrera, L., Zamora, A., Rangel, Y. (2020). *Justicia en trámite. El limbo de las investigaciones sobre violencia digital en México.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2024/10/Luchadoras_JusticiaEnTramite.pdf

83. Instituto Nacional de Estadística y Geografía. (2025). *Módulo sobre Ciberacoso (MOCIBA) 2024.* https://www.inegi.org.mx/contenidos/programas/mociba/2024/doc/mociba2024_resultados.pdf

84. ONU Mujeres. (2025). *Violencia digital contra las mujeres y las niñas.* https://mexico.unwomen.org/sites/default/files/2025-12/onu_mujeres_mexico_brief_violencia_digital_101125.pdf

85. ONU Mujeres. (2025). *Violencia digital contra las mujeres y las niñas.* https://mexico.unwomen.org/sites/default/files/2025-12/onu_mujeres_mexico_brief_violencia_digital_101125.pdf

86. Burgess, M. (2025, July 14). Esas aplicaciones que "desnudan" gente con IA están generando 36 millones de dólares al año. *Wired*. https://es.wired.com/articulos/esas-aplicaciones-que-desnudan-gente-con-ia-estan-generando-36-millones-de-dolares-al-ano

87. EFE. (2024, January 24). Ciudad Juárez, primer lugar en producción de videos sobre abuso sexual infantil. *El Financiero.* https://www.elfinanciero.com.mx/nacional/2024/01/24/ciudad-juarez-primer-lugar-en-produccion-de-videos-sobre-abuso-sexual-infantil/

88. EFE. (2025, July 16). Trata por material de abuso de menores en México sube 86 % en primer trimestre 2025. *SWI swissinfo.ch.* https://www.swissinfo.ch/spa/trata-por-material-de-abuso-de-menores-en-m%C3%A9xico-sube-86-%25-en-primer-trimestre-2025/89686591

89. Rodríguez. A. (2025, May 23). Sentenciado a cinco años de prisión Diego N, ex alumno del IPN, por el delito de pornografía infantil. *El País.* https://elpais.com/mexico/2025-05-23/sentenciado-a-cinco-anos-de-prision-diego-n-ex-alumno-del-ipn-por-el-delito-de-pornografia-infantil.html

90. Rodríguez, A. (2025, November 11). Al menos 400 alumnas de secundaria denuncian la alteración de sus fotos con IA para fines pornográficos en Zacatecas. *El País.* https://elpais.com/mexico/2025-11-11/al-menos-400-alumnas-de-secundaria-denuncian-la-alteracion-de-sus-fotos-con-ia-para-fines-pornograficos-en-zacatecas.html

91. Orden Jurídico de México. (n.d). *Ficha técnica Ley Olimpia*. https://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

92. Escobar, C. & Trujano, M. (2023, April 25). Sentencias por "Ley Olimpia", en 1% de los casos investigados. *Serendipia*. https://serendipia.digital/violencia-contra-las-mujeres/sentencias-por-ley-olimpia/

93. Cámara de Diputados del H. Congreso de la Unión. (2007, February 1). *Ley general de acceso de las mujeres a una vida libre de violencia*. Latest published amendment DOF 15-01-2026 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf

94. Cámara de Diputados del H. Congreso de la Unión. (2021, June 1). *Código penal federal.* https://www.diputados.gob.mx/LeyesBiblio/ref/cpf/CPF_ref150_01jun21.pdf

95. Cámara de Diputados del H. Congreso de la Unión. (2012, June 14). *Ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos*. Latest published amendment DOF 19-01-2018 https://www.gob.mx/indesol/documentos/ley-general-para-prevenir-sancionar-y-erradicar-los-delitos-en-materia-de-trata-de-personas-y

96. Avendaño, E., Contreras, A., Macías, G., Paéz, S., Rivera, K., Samperí, A., Soria, E., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

97. Te protejo México, (n.d.) *Marco legislativo del material de abuso sexual infantil federal y estatal de México.* https://teprotejomexico.org/wp-content/uploads/sites/2/2025/02/marco-legislativo-tpm.pdf

98. Te protejo México, (n.d.) *Marco legislativo del material de abuso sexual infantil federal y estatal de México.* https://teprotejomexico.org/wp-content/uploads/sites/2/2025/02/marco-legislativo-tpm.pdf

99. Suprema Corte de Justicia de la Nación. (2023). *Protocolo para juzgar con perspectiva de género.* https://www.scjn.gob.mx/derechos-humanos/sites/default/files/protocolos/archivos/2020-11/Protocolo%20para%20juzgar%20con%20perspectiva%20de%20g%C3%A9nero%20%28191120%29.pdf

100. Samperí, A., Contreras, A., Avendaño, E., Soria, E., Macías, G., Rivera, K., Paéz, S., & Valerio, S. (2025). *Una mirada crítica feminista al delito de difusión de contenido íntimo sin consentimiento.* Luchadoras. https://luchadoras.mx/wp-content/uploads/2025/03/InformeJuridico_Luchadoras_1.pdf

101. Cámara de Diputados del H. Congreso de la Unión. (1928, May 26, July 14, August 31). *Código Civil Federal*. DOF 14-11-2025. https://mexico.justia.com/federales/codigos/codigo-civil-federal/

102. Secretaría de las Mujeres de la Ciudad de México. (n.d.). *Violencia digital*. https://semujeres.cdmx.gob.mx/violencia-digital

103. Gobierno de la Ciudad de México. (n.d.). *Línea Mujeres*. https://cms311.cdmx.gob.mx/linea-mujeres/

104. Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes. (n.d.). *SIPINNA Estado de México*. https://sipinna.edomex.gob.mx/sipinna_nacional

105. For additional information, see: https://cultivandogeneroac.org/

106. For additional information, see: https://defensorasdigitales.org/

107. For additional information, see: https://hijasdeinternet.org/

108. For additional information, see: https://luchadoras.mx/

109. For additional information, see: https://socialtic.org/

110. Escobar, C. & Trujano, M. (2023, April 23). Sentencias por "Ley Olimpia", en 1% de los casos investigados. *Serendipia.* https://serendipia.digital/violencia-contra-las-mujeres/sentencias-por-ley-olimpia/

111. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

112. Rojas, D. & Del Pozo, C. (2026). *Gender-Based Disinformation & Deepnudes in Mexico.* Friedrich-Naumann Stiftung für die Freiheit. https://shop.freiheit.org/#!/Publikation/2085

113. Cámara de Diputados del H. Congreso de la Unión. (2019, September 30). *Ley general de educación.* Latest published amendment DOF 15-01-2026 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGE.pdf

AI use disclosure : AI tools were used solely for writing purposes, namely language editing and rephrasing.



IVADO

EON INSTITUTE

with the support of

CANADA FIRST RESEARCH EXCELLENCE FUND

APOGÉE CANADA FONDS D'EXCELLENCE EN RECHERCHE