Protecting the Digital Generation: Advancing Public-Private Action Against AI-Driven Trafficking of Women and Youth

Jaewon Choi (South Korea, USA) , Alexa Dominique Pascual (USA), Tae Kyu Lee (USA), Lily Yangliu (Canada), Isaiah Jones (USA), Pim van Benthem (Netherlands) DMUN Foundation

June 18, 2025

Executive Summary

The application of Artificial Intelligence (AI) now stands at the forefront of strategies aimed at combating human trafficking and violence. AI serves two functions in global security by creating both opportunities and risks. The adverse effects of artificial intelligence are increasingly recognized, especially its role in online exploitation and human trafficking. The protection of children and young people in digital environments has become a significant policy and research challenge that continues to develop.

AI has the potential to enhance detection and prevention systems; however, traffickers and perpetrators also utilize AI to scale, speed up, and sophisticate their online operations. Researchers have found that every year, one in eight children around the world suffers from some type of online sexual abuse or exploitation. Modern AI systems generate synthetic child sexual abuse material (CSAM) while also automating grooming procedures and developing convincing fake identities alongside realistic content.[1] By 2023, reports from the U.S. National Center for Missing & Exploited Children cited 4,700 AI-created CSAM cases, while the UK's Internet Watch Foundation noted a dramatic 380% rise in this material, with young girls being the primary victims.

Technologies enhanced by artificial intelligence help facilitate the digital recruitment of trafficking victims. The initial contact between traffickers and over half of domestic minor sex trafficking survivors took place on online platforms where AI technologies are increasingly used to boost profiles and messaging. The volume of reported child exploitation cases is straining existing systems:[2] In 2023, the U.S. CyberTipline registered 36.2 million suspect child sexual exploitation reports, while experts worry about AI-made false material impeding real case detection.

This report combines current data and trends about the role of AI in online youth exploitation by utilizing recent academic studies, international organization reports and operational insights from child protection and anti-trafficking networks. The report examines how these technological advancements impact international agreements, including the Sustainable Development Goals (SDGs), the Convention on the Rights of the Child, and the Women, Peace, and Security (WPS) agenda.

The report provides proven strategies for UN agencies and Member States to implement, with the objectives of strengthening international governance systems by promoting responsible AI development and deployment and enhancing online protections for young people. The establishment of a UN-led initiative to maintain ongoing collaboration with major social media companies represents the essential core of these recommendations. This

---

[1] https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam?
[2] https://www.missingkids.org/gethelpnow/cybertipline?

initiative seeks to stop AI misuse in human trafficking against young users and women by creating common safety standards, early-warning systems, and accountability measures across different platforms.

Introduction

As artificial intelligence (AI) technologies rapidly evolve, they are reshaping nearly every facet of our society, including the efforts to combat human trafficking and online violence. While AI offers powerful tools for enhancing detection, crime prevention, and community protection systems, it also introduces new dangers. Traffickers are increasingly leveraging AI to expand and sophisticate their operations, accelerating online exploitation with alarming scale and efficiency.

This duality of AI, both as a tool for harm and a potential safeguard, places it at the center of contemporary security and child protection discourse. The growing prevalence of synthetic child sex abuse material (CSAM), AI-driven grooming and manipulation tactics, and the use of convincing fake identities are just some of the ways malicious actors exploit technological progress. At the same time, law enforcement agencies, child protection services, and international organizations are seeking to harness the potent power of AI for early detection and systemic intervention.

Our report explores the complex role of AI in online youth exploitation. We draw from current data, academic research, and insights from global protection networks. Through a balanced examination of risks and opportunities, the report aims to inform and guide UN agencies and Member States in shaping effective, ethical, and forward-looking responses.

This issue also closely intersects with the Women, Peace, and Security (WPS) agenda, which emphasizes the importance of protecting women and girls from violence and ensuring their participation in security and policy-making. AI-facilitated online trafficking disproportionately affects women and girls. Women and girls face the highest risk from online trafficking, which uses AI to exploit them sexually through deepfake pornography and digital recruitment on social media, along with AI-enabled grooming.[3] The development of new threats weakens international actions against gender-based violence and puts into question the obligations established in UN Security Council Resolution 1325 and its subsequent resolutions. Given that the digital space is becoming a highly competitive field, we must adopt gender-sensitive approaches to AI governance, as well as cybersecurity and anti-trafficking policies, to protect the rights and self-determination of women and girls globally.

In highlighting these urgent challenges and opportunities, this report seeks to catalyze cross-sectoral action and policy innovation to ensure that emerging technologies are aligned with international human rights frameworks and serve the security and dignity of all individuals—especially the most vulnerable.

---

[3] https://unidir.org/files/2021-09/UNIDIR_System_Update.pdf?

Background and Context

The digital world presents escalating dangers, which now represent the leading risky environments for susceptible groups, including young people and women. Artificial intelligence (AI) supports safety tool development, but exploitative networks are increasingly adopting it to attack young people online. The generation of deepfakes has led to more automated grooming strategies, while synthetic child sexual abuse material (CSAM) production continues to grow as these methods evade current detection techniques. Technological dangers, alongside fundamental human threats, erode the trust and personal security of countless young people, including young women.

The United Nations' digital safety and anti-trafficking frameworks demonstrate progress, but it has yet to establish a coordinated system to combat AI-driven online exploitation of youth and women. The current directives show a tendency to address technology governance and gender-based violence separately without tackling their critical intersection. Young users, who make up the majority of global internet users, face a higher risk of exposure to dangers.

The United Nations needs to create a new public-private partnership platform that brings together multiple stakeholders to protect women and young people from AI-enabled online trafficking. This platform will emerge from a collaboration between major technology firms, including Meta and X, as well as the United Nations' global policy framework.
* Early-warning systems should be established to detect digital trafficking threats that target youth.
* Establish AI safety regulations for platforms commonly accessed by young users and monitor their implementation to ensure compliance.
* Enable organizations led by young people and survivors to work collaboratively on designing intervention strategies.
* The platform should focus on gender-based dangers that stem from biased algorithms, which expose users to detrimental content or facilitate digital trafficking recruitment processes.
The United Nations currently lacks this partnership model, yet requires it immediately. The online environment will remain extremely dangerous for future generations unless protective measures are established. The United Nations has the opportunity to pioneer protective measures that focus on future developments and the needs of young people while upholding human rights principles.

Key Findings and Issues Identified

AI Generated CSAM
    a. Mass generation of realistic material
        i. The Internet Watch Foundation (IWF) detected over 3,500 AI-generated child sexual abuse images in a single 30-day review, signalling a 17% increase from previous months. The IWF also found that the majority of the AI-generated images depicted the most severe "Category A" abuse.[4]
    b. AI-trained on illicit datasets
        i. A Stanford Internet Observatory report found that AI models like Stable Diffusion had been trained on thousands of real CSAM images from the LAION dataset, an index of online images that has been used to train AI image-makers. This enabled AI models to create convincing fake imagery.[5]
    c. Straining detection systems
        i. The United States CyberTipline received 4,700 reports of AI-generated CSAM and a total of 36.2 million child exploitation reports in 2023, which was a 12% increase from 2022. Experts warn that AI-flooded systems hamper efforts to isolate genuine cases.[6]

Exploitation of AI by Malicious Actors
    a. Synthetic grooming and deception
        i. Offenders are using AI to create virtual identities, automate grooming systems, and craft realistic fake profiles for targeting minors through online platforms.[7]
    b. Online trafficking recruitment
        i. AI-enhanced platforms and messaging tools significantly aid traffickers. More than half of domestic minor sex trafficking survivors were first contacted online, often through AI-boosted spam or messaging campaigns.[8]

AI Usage in Detection and Prevention: Potential and Gaps
    a. Advanced detection tools

[4] https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/?
[5] https://apnews.com/article/generative-ai-illegal-images-child-abuse-3081a81fa79e2a39b67c11201cfd085f
[6] https://www.theguardian.com/technology/article/2024/jul/18/ai-generated-images-child-predators?
[7] https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf
[8] https://arxiv.org/abs/2311.13118

      i.   Research shows multiple AI-based technological approaches, such as NLP (natural language processing) for trafficking ad analysis, automated CSAM classifiers with around 90% accuracy, and abuse report automation tools, that aid law enforcement efforts and reduce human exposure.

   b. Evidence limitations

      i.   A 2025 rapid evidence assessment reviewed 33 empirical studies on AI applications in child sexual abuse. All focused on prevention and detection, with zero studies examining how traffickers exploit AI.[9]

   c. Bias and interpretability concerns

      i.   Studies on trafficking detection algorithms reveal strong potential but also significant bias risks. As such, interpretable and unbiased models are essential prior to deploying AI usage.
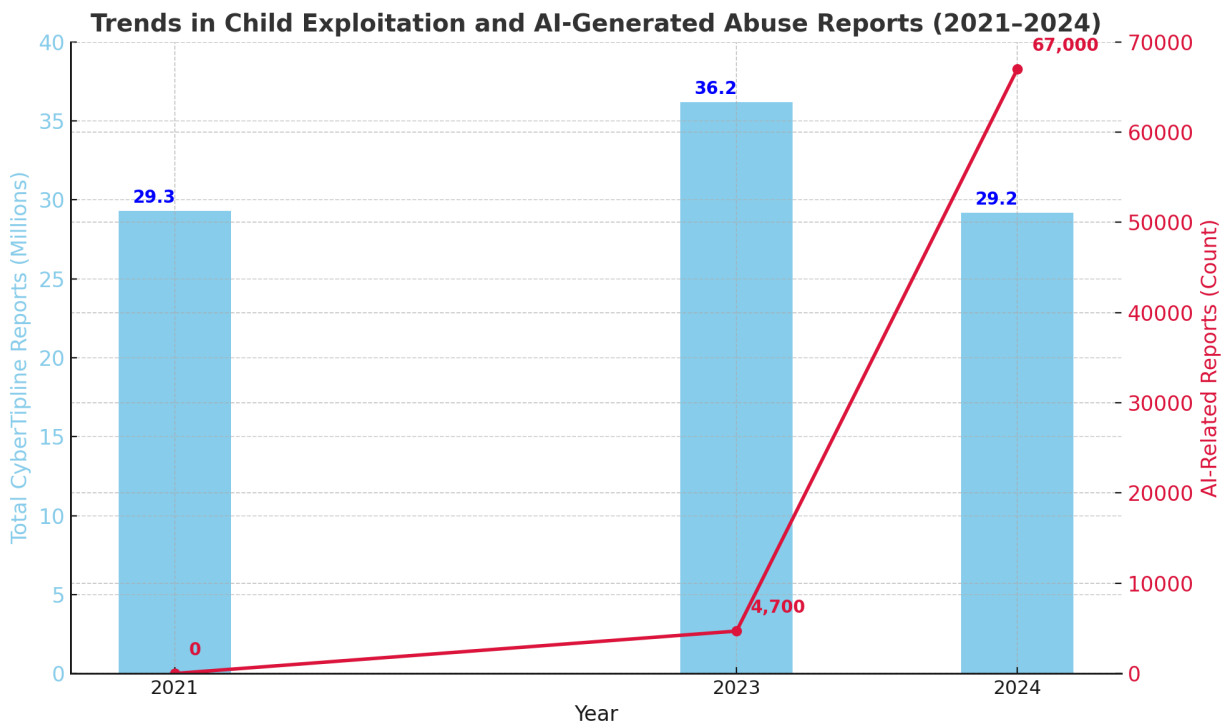
Legal, Ethical, and Systemic Shortcomings

   a. Surveillance vs privacy tensions

      i.   EU proposals such as "Chat Control 2.0" raise privacy concerns: scanning encrypted communications could violate user rights and lead to surveillance on civil society.[10]

   b. Operational overload

      i.   Law enforcement systems like CyberTipline (U.S) are overwhelmed by insufficient metadata, old infrastructure, and lack of enhancement to filter AI-generated noise.[11]

[9]https://www.researchgate.net/publication/388275053_Artificial_intelligence_and_child_sexual_abuse_A_rapid_evidence_assessment

[10]https://www.lemonde.fr/en/les-decodeurs/article/2023/09/26/the-eu-fight-against-child-pornography-stokes-fears-of-widespread-online-surveillance_6140055_8.html

[11]https://apnews.com/article/cybertipline-child-sexual-abuse-stanford-23436c59d8aa03aa3d173ed5b63f8bfd

Trends in Child Exploitation and AI-Generated Abuse Reports (2021–2024)

This chart compares the total number of child exploitation reports submitted to the U.S. CyberTipline from 2021 to 2024 with the dramatic rise in AI-generated abuse reports. While overall reporting remained consistently high, AI-related cases surged from 4,700 in 2023 to 67,000 in 2024—a 1,325% increase—highlighting the urgent need for new safeguards in digital child protection.

Recommendations

1. The United Nations should establish an official task force that brings together multiple stakeholders to address AI and online safety.

Objective:
The United Nations must establish a dedicated task force under the Office of the Secretary-General's Envoy on Technology or through the United Nations Office on Drugs and Crime (UNODC), focusing on stopping AI-enabled exploitation. The proposed task force will enhance UN methods to combat AI misuse, especially as it relates to online human trafficking of women and young people. The initiative would boost private sector engagement, leading to stronger policy development, which protects youth from digital exploitation.

Participants:
Participants in the task force included leading technology firms, such as Meta and Google, alongside civil society organizations and survivor advocates from Member States, as well as AI policy experts.

Functions:

Create collective guidelines to ensure AI protection and prevent its misuse.

Identify and mitigate emerging technological risks.

Establish quick response mechanisms to combat online trafficking networks and synthetic child sexual abuse material (CSAM).

Benefits to the Private Sector:

The organization strengthens its trustworthiness and legitimacy through collaboration with a UN-supported program.

Shows ethical AI governance leadership through adherence to ESG (Environmental, Social, Governance) and CSR (Corporate Social Responsibility) standards.

Provides an advanced understanding of global regulatory developments and assists in defining standards for AI applications and content moderation practices worldwide.

Supports harmonized global frameworks to reduce the risks associated with regulatory fragmentation.

Benefits to the UN:

1. Provides the UN with enhanced technical capabilities through access to cutting-edge AI tools alongside detection algorithms and platform data.

Real-time collaboration enables more rapid responses to online exploitation and the dissemination of child sexual abuse material (CSAM).

UN policies shape platform design, which strengthens protective measures for both women and young people. The United Nations establishes itself as the leading authority in ethical digital governance while shaping international standards for AI safety and online protection.

Implementation:

The UN already has multiple entities that can support or house this task force. The Office of the Secretary-General's Envoy on Technology is the natural convener, given its mandate on digital cooperation. The United Nations Office on Drugs and Crime (UNODC) has deep expertise in fighting human trafficking and cybercrime, while UNICEF focuses on child protection. The High-Level Advisory Body on Artificial Intelligence can provide a foundation of expertise and experience to draw upon.

Formal Mandate: The Secretary-General's Office should issue a formal mandate creating the "Task Force on AI and Online Safety," co-chaired by the Tech Envoy and the Executive Director of UNODC. This will provide both technological and criminal justice leadership to give the formal mandate the power it needs.

Stakeholder Onboarding: Actively recruit the proposed participants: technology firms like Meta and Google, civil society organizations (e.g., ECPAT, Thorn), survivor-advocate networks and youth networks. The UN's convening power is its greatest asset here and can play to its strength .

Develop a Charter: The first task of this body should be to create a charter outlining its functions: establishing shared safety principles, creating a rapid-response protocol for emerging threats like new forms of synthetic media, and defining a work plan.

2. Begin a joint Public-Private "Safe AI for Youth and Women" Initiative

Framework:
This initiative aligns with the UN Global Compact's framework to promote ethical AI practices and digital safety measures.

Mandate:
Establish universal AI governance rules for social media platforms, which should consist of the following:

AI transparency and independent audit mechanisms.
Social media content moderation systems must be adapted to protect users against gender-based violence and grooming dangers.

Funding:
This initiative is a prime candidate for a multi-donor trust fund managed by the UN Multi-Partner Trust Fund Office (MPTFO). Private sector partners and international donors like the Gates Foundation or Ford Foundation could be major contributors.

3. Develop advanced Data Sharing Protocols along with Joint Investigative Tools.
Develop a UN–Tech Protocol that enables the safe, rights-focused, and anonymous sharing of platform data for supporting trafficking investigations.
Develop AI tools together with private companies to detect grooming behaviours and trafficking networks alongside synthetically produced exploitative content.

Implementation:
UNODC and INTERPOL (a close UN partner) have existing protocols for international criminal investigations. UN Global Pulse, the Secretary-General's innovation lab, has expertise in data privacy and analytics that can be used to build a framework.

Funding:
Projects could be funded through the UN Trust Fund for Victims of Human Trafficking or through specific grants from Member States' justice and interior departments of these states.

4. All UN policy discussions related to AI and digital safety must include youth representation and women's rights advocates.
All UN policy discussions related to AI, digital safety, and platform accountability must include representatives from youth and women's rights organizations.

Justification:
AI-enabled exploitation impacts women and youth more than other groups, yet these groups see little representation in policymaking circles.

Implementation:
The Office of the Secretary-General's Envoy on Youth is the primary vehicle for this. The UN also has a strong tradition of including civil society, but this recommendation calls for formalizing youth roles specifically. Therefore, establishing a Formal Youth Advisory Body on AI & Digital Safety would be a useful option: As recommended, this permanent group, managed by the Youth Envoy's office, would serve as a consultation body for all other UN AI initiatives.

Mandate Youth Seats and fund participation:
The terms of reference for this new AI Task Force, the Digital Safety Forum, and other relevant bodies all must include dedicated seats for representatives from the Youth Advisory Body and leading women's rights organizations. The UN must also allocate funds to support the travel and participation of these representatives to ensure that inclusion is meaningful and not limited by financial constraints of the members.

Funding:
This aligns perfectly with the UN's Youth 2030 strategy plan. The Generation Equality Forum, led by UN Women, is a model for multi-stakeholder engagement that can be taken as inspiration. The UNICEF Innovation Fund and UN Women's Fund for Gender Equality could be tapped to support youth-led research and participation in these kinds of forums.

5. Introduce a UN Platform Accountability Scorecard
Publish yearly evaluations through an "AI & Online Safety Scorecard" that assesses tech companies based on the following:
Preventing AI misuse
Transparency in AI deployment and enforcement
Addressing gendered and youth-targeted exploitation

Purpose: The purpose of this measure is to reward accountable AI management while increasing transparency and identifying top-performing platforms.

Implementation:
The UN has a long and successful history of using flagship reports and indices (like the UNDP's Human Development Index) to create global benchmarks and drive policy change. This is a core quality that it can leverage.

The UN Task Force proposed in Recommendation 1 should be mandated to develop the specific metrics for the "AI & Online Safety Scorecard". These metrics must be transparent, measurable, and based on the criteria listed in the report: preventing AI misuse, transparency in AI deployment, and enforcement against exploitation of any kind.

To ensure clear credibility, the data for the scorecard should be collected and analyzed by an independent body, which could potentially be a consortium of academic institutions and civil society experts, in partnership with the UN and partners.

The scorecard's annual release should be a major event, timed to coincide with the proposed Global Digital Safety Forum to maximize media attention, political pressure and impact.

Funding:
The research and data analysis for the scorecard could be funded through dedicated grants for digital governance and human rights projects. Philanthropic foundations focused on technology and society would be likely funders that would support this project.

6. Convene a Global Digital Safety Forum

Organize a yearly UN summit to unite representatives from private sector leadership, government stakeholders, and civil society representatives alongside youth organizations.

Demonstrate new developments in digital protections while reviewing advancements in policy execution.

The Global Digital Safety Forum could receive support from UN Women, UNICEF, the Office of the Envoy's Tech Envoy, and ECOSOC as co-hosting organizations.

Implementation:

The UN is the world's premier convener. It has extensive experience organizing large-scale summits. The report suggests that UN Women, UNICEF, the Office of the Tech Envoy, and ECOSOC could be co-hosting and supporting organizations, which would provide significant institutional weight for this.

The first step would be to get formal buy-in from the leadership of the proposed co-hosts (UN Women, UNICEF, etc.) to establish a steering committee for the forum. The forum is best to have a standing agenda that includes the official release of the UN Platform Accountability Scorecard, a review of the AI Task Force's progress, and sessions dedicated to youth-led solutions evaluating the project. The forum's budget should include dedicated funding to ensure meaningful participation from youth representatives and survivor advocates from diverse backgrounds, as called for in Recommendation 4.

Funding:

The forum could be financed through a multi-stakeholder model, with contributions from host countries and their state departments, sponsoring Member States, and private sector partners as part of their CSR and ESG commitments.

Strategic Rationale

Current national laws and corporate moderation systems are insufficient to manage the global scale and complexity of AI-driven online exploitation. [12]The 1,325% surge in AI-generated child sexual abuse material from 4,700 reports in 2023 to 67,000 in 2024 demonstrates the urgent need for systemic safeguards. Fragmented regulations and inconsistent platform responses allow traffickers and exploiters to evade detection and operate across jurisdictions.

The recommendations target existing governance gaps because states and companies cannot individually address the extensive scale and complexity of AI-driven online exploitation. A formal UN platform for

---

[12] https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam?utm_

cooperation would enhance collective accountability and actions, making digital environments safer for vulnerable groups, including youth and women.

Economic Impact

Another critical, yet less-discussed aspect of AI-facilitated trafficking and exploitation is the economic impact. The ILO estimates that trafficking in human beings and forced sexual exploitation generate over USD 150 billion annually in illegal profits. This deprives domestic economies of valuable financial resources and contributes to fiscal instability by diminishing tax bases, impairing domestic resource mobilization, and distorting market competition. Furthermore, the high costs associated with law enforcement and criminal justice responses, coupled with the loss of human capital, reduce the overall economic productivity of affected nations.

Therefore, it is important to highlight that the strengthening of digital safety and AI governance can also be seen as an economically sound investment. By investing in online safety, governments can reduce enforcement costs, improve financial system resilience against cybercrime, and foster a secure environment for trade, e-commerce, and digital innovation. Curbing trafficking and exploitation also enhances Member States' creditworthiness, attracts sustainable investment, and bolsters their long-term growth potential.

At the global level, adopting harmonized safeguards can also support greater coherence in regulatory environments and reduce compliance costs for technology companies operating across borders. Public-private partnerships and resource pooling for AI safety measures can also lead to shared value creation, where firms gain reputational trust and governments benefit from fiscal space. In this way, online safety for women and youth not only supports SDG 16 and SDG 17 but also aligns with and strengthens the Addis Ababa Action Agenda on Financing for Development by advancing the fight against illicit financial flows and helping to mobilize resources for inclusive growth. Ultimately, advancing AI safety is not only a moral imperative but also a strategic investment that delivers shared returns—protecting vulnerable populations, strengthening state stability, and enabling companies to thrive in a trusted and sustainable digital economy.

Youth Stakeholder Participation in AI Governance

As digital platform users, young people face significant exposure to AI-enabled threats such as grooming and trafficking. Although young people stand at the heart of this crisis, they rarely get involved in creating solutions. AI governance requires effectiveness and inclusivity, which can be achieved by actively involving young users and incorporating youth leadership throughout multilateral decision-making processes.

Young people today are among the most active users of digital platforms—and the most vulnerable to AI-enabled online threats, including grooming, trafficking, and gender-based violence. Yet, despite being at the center of this crisis, youth are rarely included in designing the solutions. For AI governance to be effective, safe, and inclusive, it must center the voices of young users and integrate youth leadership into every level of decision-making within the multilateral system.

Key Recommendations for Youth Inclusion:

Establish a United Nations Youth Advisory Body to address artificial intelligence and digital security issues. The Office of the Secretary-General's Envoy on Youth or the Tech Envoy should establish a permanent advisory group composed of youth leaders and advocates. This body should:

1. Guide the dangers young users encounter from AI-generated content and threats such as online grooming and synthetic sexual abuse material.

2. Young people should be empowered to develop policy solutions that address online dangers through United Nations action.

The advisory body must include members from different geographical areas and genders, with particular attention to groups that face disproportionate impacts.

3. All UN AI governance bodies, Office of the Secretary-General's Envoy on Technology, High-Level Advisory Body on Artificial Intelligence (UN AI Advisory Body, International Telecommunication Union (ITU), UNESCO (United Nations Educational, Scientific and Cultural Organization), UN Human Rights Council / OHCHR, United Nations Interagency Working Group on AI, Global Digital Compact (GDC), UN Global Pulse must include youth representation.

4. All United Nations task forces, summits, and working groups focusing on AI, as well as digital rights and online protection, must incorporate youth representatives who engage actively rather than merely undergo symbolic consultation.

5. Positions on the proposed UN AI Task Force and Digital Safety Forum must be established.

6. Youth should engage in developing standards for AI audits while promoting transparency and platform regulation.

Fund Youth-Led Research and Digital Protection Projects

Establish specialized funding programs to support organizations and researchers led by young people who focus on AI-related threats. Priority should be given to:

1. Research initiatives are dedicated to investigating AI applications which target young people online.

2. Digital technologies enable community-driven interventions to combat misinformation as well as trafficking and gender-based violence.

Formalize consistent international youth forums to discuss AI-related dangers.
UNICEF, UN Women, and the Tech Envoy's Office should organize ongoing global consultations involving youth and student networks to develop policies on AI safety and responsible innovation.

Why This Is Urgent:

Youth users, who make up the majority of the audience on TikTok, Instagram, and YouTube, are increasingly facing dangers from manipulated deepfakes and predatory algorithms created by AI systems. Policymaking bodies regulating AI often show a lack of significant representation from the majority of users who comprise these platforms. Global governance frameworks will become disconnected from reality and ineffective without youth involvement.

Youth engagement goes beyond protection as it acknowledges their role as digital rights holders and key contributors who drive toward a safer AI future with equity.

Conclusion

The speedy evolution of AI presents a dual reality: While it hands us powerful tools for protection, it can also be weaponized to escalate the online exploitation of women and youth on an unprecedented scale. This report has illuminated the alarming surge in AI-driven trafficking, grooming, and the creation of synthetic child sexual abuse material (CSAM), which are overwhelming current legal and operational frameworks. The statistics are shocking, with AI-generated CSAM cases rising dramatically, showing a clear and present danger to the digital generation.

Current national and corporate efforts are proving insufficient to counter the sophistication and scale of these growing threats. The fragmentation of regulations and inconsistent enforcement across platforms creates vulnerabilities that malicious actors can exploit. This reality underscores the urgent need for a coordinated,

global response that bridges the gap between technology governance and the protection of human rights in the broader sense, particularly for women and young people who are disproportionately affected.

The recommendations outlined in this report offer a strategic path forward. At their core is the call for a UN-led, multi-stakeholder collaboration that brings together technology companies, Member States, civil societies, and critically also the voices of youth and survivors who have been affected by this. By establishing a dedicated task force as such, launching a "Safe AI for Youth and Women" initiative, and developing shared protocols and policies for data and investigation, the international community can create a united front against digital exploitation to safeguard the vulnerable.

Implementing these measures will not only enhance our collective ability to respond to immediate threats but also create a culture of responsible innovation and corporate accountability. The United Nations is uniquely positioned to lead this global effort, aligning technological advancement with the enduring principles of human rights, security, and dignity for all those affected. The time for isolated and focused action is over; a unified, forward-looking and long-term strategy is essential to reclaim the digital space as a safe environment for all future generations to come.