MENA WORKSHOP

TECH FACILITATED SEXUAL EXPLOITATION AND ABUSE OF CHILDREN

ديجي آمن

ⴷⵉⴳⵉ ⴰⵎⵉⵏ

DIGI-AMEN

Rabat - Morocco
5th, 6th, 7th May 2025

ACKNOWLEDGEMENTS

ECPAT International , Amane , Bayti extend their gratitude to all individuals and organizations involved in this workshop.

ORGANIZATIONS INVOLVED:

EGYPT

- EGYPTIAN FOUNDATION FOR THE ADVANCEMENT OF THE CHILDHOOD CONDITION
- SPEAK UP

MAURITANIA

- ASSOCIATION MAURITANIENNE POUR LA SANTÉ DE LA MÈRE ET DE L'ENFANT

MOROCCO

- AMANE
- BAYTI
- AI.BI
- DROIT ET JUSTICE
- AICEED
- FONDATION RITA ZNIBER
- 100% MAMANS
- AAUPE TANGER
- OVCI
- SOS VILLAGE D’ENFANTS
- CASA LAHNINA
- KIF MAMA KIF BABA
- ASSOCIATION MEDIA ET CULTURE
- AMNA
- EEACC
- NADA
- INSAF
- NAHDA
- PROGETTO MONDO
- OUSRATU
- AIDA

TUNISIA

- VISIONS OF THE FUTURE

SUDAN

- NADAAK AZHAR

The opinions expressed in this workshop are solely those of ECPAT international and Amane and do not necessarily reflect the views of partner organizations.

THE WORKSHOP WAS FUNDED BY AEGIS.

WORKSHOP FACILITATED BY:

Sara El Ouedrhiri , Hassan Tabikh , Salla Huikri

SUGGESTED CITATION:

ECPAT International. (2025). TECH FACILITATED SEXUAL EXPLOITATION AND ABUSE OF CHILDREN

ECPAT International

EXECUTIVE SUMMARY

This report outlines the key outcomes, discussions, and recommendations from the **regional workshop on Technology-Facilitated Child Sexual Exploitation and Abuse** (TF-CSEA), organized by **ECPAT International** in collaboration with **Association AMANE** and **Association Bayti**. Held in **Rabat, Morocco**, from **May 5th to 7th, 2025**, the event gathered 23 participants from 18 NGOs across 5 countries. It aimed to strengthen civil society capacities in understanding and addressing TF-CSEA through peer learning, advocacy strategizing, and regional cooperation. Discussions highlighted both the opportunities and risks of children's growing digital access, with a focus on safeguarding practices, awareness-raising, and cross-border collaboration.

TABLE OF CONTENTS

INTRODUCTION

Over the past decades, the global community has achieved considerable progress in strengthening child protection systems and preventing various forms of violence against children. Despite these advances, the digital transformation of societies has introduced complex and rapidly evolving threats. One of the most pressing challenges today is technology-facilitated child sexual exploitation and abuse (TF-CSEA).

Unlike traditional forms of abuse, TF-CSEA leverages digital platforms and tools to reach, groom, manipulate, and exploit children. The anonymity, accessibility, and global reach of the internet allow perpetrators to target children at unprecedented scale and speed, blurring the lines between online and offline abuse and exacerbating its spread and impact.

In North Africa, the risks associated with TF-CSEA are magnified by several contextual factors: cultural taboos around discussing sexual violence, limited digital literacy among both children and adults, fragmented legal protection policies, and a lack of institutional capacity to monitor and respond to online threats. In this setting, civil society organizations play a crucial role in both prevention and response efforts, yet they too face challenges related to technical knowledge, funding, and coordination.

Recognizing the urgency of this issue, ECPAT International, in collaboration with Amane – Association Meilleur Avenir pour Nos Enfants and Association Bayti, convened a regional workshop in Rabat, Morocco, from May 5th to 7th, 2025. This workshop brought together 23 civil society representatives from Morocco, Tunisia, Algeria, Mauritania, Egypt, Libya, and Sudan to deepen regional understanding of TF-CSEA, strengthen cross-border collaboration, and support CSOs in developing effective strategies for prevention, safeguarding, and advocacy.

This workshop links to a broader, multi-year initiative led by ECPAT to strengthen CSO capacities in tackling technology-facilitated abuse across the MENA region. Building on the momentum of previous workshops held in Jordan and Tunisia, the Rabat workshop aimed to equip participants with practical tools to reinforce their internal safeguarding priorities and mechanisms and inform evidence-based advocacy aligned with the evolving digital landscape.

Through the exchange of promising practices, peer learning, and the establishment of a regional protection network, the workshop not only contributed to empowering CSOs' understanding and response mechanisms to TF-CSEA, but also contributed to the naissance and consolidation of a broader regional movement and network committed to ending technology-facilitated sexual exploitation of children.

This report documents the proceedings, findings, and outcomes of the Rabat workshop. It synthesizes insights from rich thematic discussions, case studies, and interactive sessions. It also presents the **Recommendation Paper**, a collaboratively developed advocacy tool designed to guide future action at national, regional, and international levels.

OBJECTIVES

The Rabat workshop was structured around three interlinked objectives, each carefully designed to address the multifaceted challenges of technology-facilitated child sexual exploitation and abuse (TF-CSEA) in the North African and broader MENA contexts, and to address the gaps in terms of knowledge and actions that were revealed in previous regional workshops.

What we promised/our objectives	Why	What we delivered
Build a shared, up-to-date understanding of the scope, tactics, evolving nature, and impact of TF-CSEA in the MENA region	In a digital landscape that evolves rapidly—with new platforms, trends, and tools emerging constantly—staying informed is vital for any effective intervention.	Participants explored how perpetrators leverage technology to engage in grooming, coercion, exploitation, and the creation and dissemination of child sexual abuse material. Emphasis was placed on distinguishing TF-CSEA from other forms of online violence, recognizing its complex dynamics, and identifying the mechanisms that make digital environments dangerous for children.
Build robust internal safeguarding tools to prevent TF-CESA within CSOs	Many organizations working with children have policies in place to prevent physical abuse or neglect, but fewer have comprehensive protocols that address digital risks.	Sessions explored what it means to be a “digitally safe” organization: implementing child-friendly communication practices online, securing digital data, training staff to recognize signs of online exploitation, and creating clear reporting and escalation pathways. The workshop encouraged participants to think expansively about child protection—beyond physical spaces and into virtual environments

What we promised/our objectives	Why	What we delivered
Facilitate cross-border exchange between CSOs from the MENA region on experiences and best practices in advocacy in addressing and TF-CSEA prevention.	TF-CSEA is inherently a transnational issue: perpetrators often exploit jurisdictional gaps, moving across borders digitally even if they remain physically in place. To counter this, there is a growing need for a coordinated regional approaches and action to address the issue and prevent it on a national, regional and international scale.	The workshop served as a platform for building such collaboration. Participants engaged in structured dialogue and networking to explore opportunities for joint action, knowledge-sharing, and future alliances. This spirit of regional solidarity culminated in the development of a Recommendation Paper, a collective output that reflects the diverse insights, priorities, and aspirations in terms of action and advocacy for the participants.

ORGANIZING COMMITTEE

Association Bayti is a Moroccan non-governmental organization founded in 1995 and recognized as a public utility NGO in 1999. Bayti is dedicated to protecting children in vulnerable situations—particularly those living or working on the streets—by offering shelter, psychosocial support, education, and healthcare services. Operating primarily in Casablanca, Essaouira, and Kénitra, Bayti also provides family tracing, legal assistance, and reintegration programs.

AMANE – Association Meilleur Avenir pour Nos Enfants is a Moroccan civil society organization dedicated to the promotion and protection of children's rights. Headquartered in Rabat, AMANE operates across all 12 regions of Morocco. The organization focuses on preventing violence, exploitation, and abuse against children by offering specialized training, engaging in advocacy, and supporting the development of child protection policies. AMANE collaborates closely with communities, professionals, and other civil society stakeholders to foster safe environments for children and to ensure their voices are meaningfully included in decisions that affect their lives.

ECPAT International -End Child Prostitution and Trafficking is a global network dedicated to ending the sexual exploitation of children in all its forms. Headquartered in Bangkok, Thailand, ECPAT brings together over 120 member organizations in more than 100 countries. The network works through research, advocacy, and capacity building to influence policy, strengthen child protection systems, and ensure that children everywhere are free from sexual exploitation, including trafficking, online abuse, and child marriage.

RECAP IN NUMBERS

DAYS

3 days

PARTICIPANTS

- 18 NGOs
- 23 participants
- 9 M
- 14 F

COUNTRIES

- Morocco
- Mauritania
- Tunisia
- Sudan
- Eqypt

SESSIONS

8 sessions

TOOLS CHECK-LIST

- Internal safeguarding policies
- Internal capacity building
- Social media networking
- Digital literacy
- Technical check-up
- Monitoring and evaluation for the application of digital safeguarding

COMMITMENTS

- One regional recommendation paper:
- 10 regional commitments
- 10 recommendations to national and international stakeholders
- 8 recommendations to CSOs
- 6 recommendations to the private sector

THEMATIC DISCUSSIONS

INTERNET PENETRATION IN NORTH AFRICA

The rapid growth of internet penetration in North Africa is a significant factor in shaping the digital landscape in the region. Over the past two decades, the number of internet users globally has surged from 1 billion in 2002 to an estimated 5.5 billion by 2024, reflecting the increasing global reliance on digital technologies. In North Africa, the number of internet users has also seen a dramatic rise, with notable variations between countries:

Country	2005	2022	Growth rate %
Morocco	15.1%	89.9%	74.8%
Algeria	5.8%	71%	65.2%
Mauritania	0.7%	44.4%	43.7%
Tunisia	9.7%	73.8	64.1%
Sudan	1.3%	28.7%	27.4%
Egypt	12.8%	72.2%	59.4%

This increase in internet access reflects broader social and economic shifts in the region, driven by greater access to mobile devices, broadband, and digital services. However, this expansion also brings with it heightened risks, particularly for vulnerable groups like children.

THEMATIC DISCUSSIONS

DIGITAL USAGE PATTERNS AND RISKS FOR CHILDREN

As internet access grows, so does the use of digital platforms for various purposes. Globally, the primary reasons people use the internet are:

- Information and Research 62.8%)
- Social Networking (60.2%)
- Entertainment and Media (54.7%)

While digital technologies offer many benefits, they also expose children to a range of online threats. While official regional data on the age at which children first go online or how frequently they use the internet remains unavailable, global trends provide some insight. For example, studies show that children may start using smartphones and access the internet as early as the age of 6ys. In the UK, statistics reveal that internet use among children begins as early as the age of 3ys:

CHILDREN BETWEEN 3 - 4

- 1% of children have their own smartphones.
- 10% have their own tablets.
- 96% watch TV, on average for 14 hours a week.

CHILDREN BETWEEN 5-7

- 5% of children have their own smartphone.
- 42% have their own tablet.
- 97% watch TV for an average of 13 hours a week.
- 67% go online for nearly 9 hours a week.
- 4% have a social media profile.
- 63% play games for 7 hours a week.

CHILDREN BETWEEN 8-11

- 33% have smartphones.
- 47% have tablets.
- 94% watch TV for 13 hours.
- 93% go online for nearly 13 hours a week.
- 18% have a social media profile.
- 74% play games for an average of 10 hours a week.

CHILDREN BETWEEN 12- 15

- 83% have phones.
- 50% have tablets.
- 90% watch TV for 13 hours a week.
- 99% go online for 20 hours a week.
- 69% have a social media profile.
- 76% play games for nearly 13 hours a week.

In the absence of official regional data, workshop participants noted that daily behaviours across the five countries reveal a growing reliance on technology and an increasingly early exposure of children to digital platforms. They emphasized the positive potential of digital tools, particularly in education. During the COVID-19 lockdowns, for instance, governments across the region turned heavily to online learning to ensure continuity in education. Participants also highlighted the critical role of technology in supporting inclusive education –helping children with disabilities access learning opportunities and bridging educational gaps for children living in remote or underserved areas.

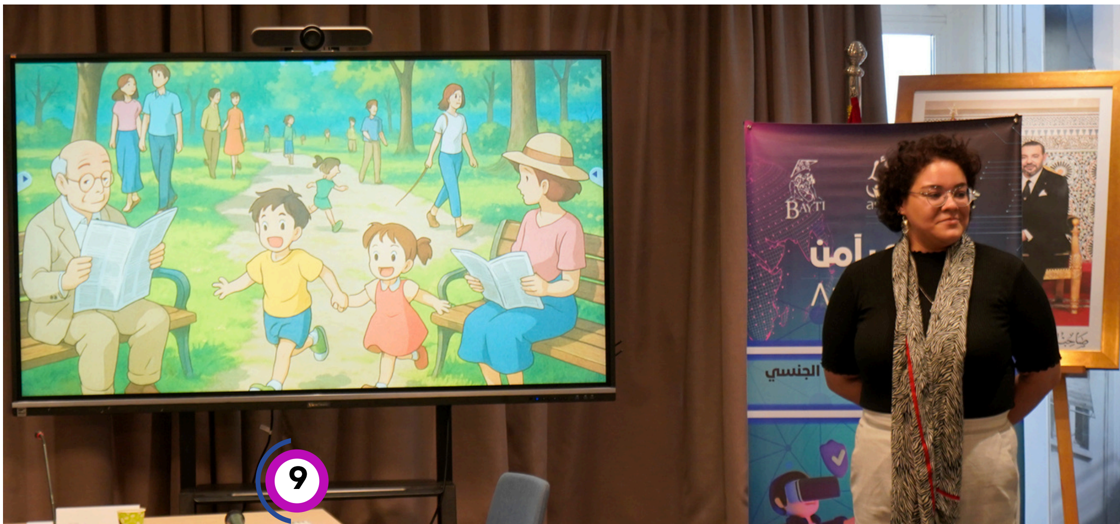
However, participants also expressed concern about the unstructured and unsupervised use of technology by children. They observed that, in many cases, parents hand over smartphones or tablets to children primarily as a means of distraction or to keep them occupied. This passive use, detached from any educational purpose, may lead to several negative outcomes.

Respectively, as children's access to digital technology increases, so too do concerns about the effects of prolonged and unstructured screen time on their emotional, cognitive, and social development. This includes:

1 - Decreased learning capacity and emerging learning difficulties

One of the most frequently cited concerns was the impact of digital saturation on learning outcomes. While educational platforms can support in/formal instruction, participants noted that many children primarily engage with technology for **passive entertainment**–watching videos, scrolling through social media, or playing games that are not cognitively stimulating. This overexposure, particularly when it replaces traditional learning methods like reading, interactive play, or verbal engagement, may lead to:

- Reduced attention spans, with children struggling to focus in classroom settings or during structured learning activities.
- Declining memory retention, especially in younger children who rely heavily on sensory and experiential learning.
- Lower academic performance, attributed to both time displacement (less time spent on homework) and the quality of engagement.



2- Reduced emotional regulation

Participants also discussed the emotional consequences of early and prolonged screen time. Unlike in-person play or family interaction, digital environments often lack emotional feedback loops. As a result, children may not develop key emotional competencies such as empathy, frustration, tolerance, or self-soothing mechanisms.

Children exposed to excessive screen time may show:

- Increased irritability or agitation, particularly when removed from devices or denied access.
- Impatience and reduced tolerance for delay which mirrors the sense of irritation when the instant gratification – that is the design of most digital platforms – is not met in real life situations.
- Mood swings or depressive symptoms, especially among pre-teens and adolescents who are exposed to online comparison culture, social validation dynamics, or inappropriate content.

In a regions where mental health support is already limited, the digital dimension compounds existing emotional and behavioral challenges. Several CSO representatives noted the rise of what could be termed as **“digital withdrawal symptoms”** –children becoming anxious, aggressive, or apathetic when disconnected from their devices.

3- Increased social isolation

Another recurring theme was the subtle erosion of interpersonal skills among children who are heavily immersed in digital spaces. While online games and social media offer a form of connection, they remain a poor substitute for face-to-face interaction, especially for younger children who are still learning how to read non-verbal cues, build empathy, and negotiate conflict.

Participants observed that:

- Many children are less inclined to participate in group activities, preferring solitary screen time.
- Peer relationships are becoming increasingly mediated by online communication, reducing opportunities for organic, in-person connection.
- Some children, especially in urban contexts, are losing interest in outdoor play or creative group-based activities.

4- Parental practices and lack of supervision

Another key point of concern discussed during the workshop was the role of paternal behaviour and digital literacy. In many cases, parents—either due to time constraints, lack of awareness, or digital inexperience—offer children mobile devices as a form of distraction. This “digital pacifier” approach, results in unstructured and unmonitored access to potentially harmful online environments. Participants underscored that many parents are unaware of the platforms their children use, the risks involved, or how to set up basic privacy protections.

THEMATIC DISCUSSIONS

EMERGING ONLINE THREATS AND DIGITAL VULNERABILITIES

In addition to concerns about developmental impacts, participants highlighted a growing range of online dangers that children face as they spend more time in digital spaces. These include cyberbullying, exploitation through false promises, and exposure to extremist ideologies. These risks become particularly concerning and get exacerbated as participants pointed to the absence of digital literacy programs in the context of the region and low adult supervision and positive practices.

a. Cyberbullying

Cyberbullying emerged as a significant and widely recognized threat discussed by participants. Defined as the use of digital platforms—such as messaging apps, gaming networks, and social media—to intimidate, harass, or isolate others, cyberbullying can have devastating psychological effects on children and adolescents.

Participants noted that in the regional context, cyberbullying often goes undetected and unreported, largely due to cultural taboos around speaking up, weak reporting systems, and a general lack of awareness among adults. Forms of cyberbullying discussed include:

- Name-calling and personal attacks through text, memes, or public posts
- Spreading rumors or false information to damage reputation
- Exclusion from online communities, such as chat groups or multiplayer games
- Threats and coercion, including extortion and manipulation

b. Exploitation through fake opportunities and promises of fame

Another emerging threat discussed was the increasing trend of online grooming through false promises—such as offers to become social media influencers, models, or gaming content creators. These predatory tactics often appeal to children's desire for recognition, success, or financial independence. Another facette of this threat is the grooming of children for financial opportunities that involve online trading, gaming tokens and fake bursary chances.

c. Radicalization and online extremism

Though less discussed in child protection circles, the issue of online radicalization was taken seriously by participants, who described it as a growing concern in the region. Children and youth—especially those feeling socially excluded, politically disillusioned, or emotionally isolated—can be targeted by extremist groups using sophisticated online grooming techniques.

The process of radicalization may involve:

- Emotional manipulation, using stories of injustice, marginalization, or persecution
- Creation of a binary worldview, dividing the world into “us vs. them”
- Gradual desensitization to violence, through videos, narratives, and community reinforcement

Participants agreed that early exposure to radical ideologies, particularly in unmoderated online spaces like forums and gaming communities, can have serious implications for public safety, community cohesion, and children’s well-being. They also highlighted the absence of positive digital narratives, digital resilience training, or culturally relevant counter-extremism content as major gaps.

THEMATIC DISCUSSIONS

UNDERSTANDING TECHNOLOGY-FACILITATED CHILD SEXUAL EXPLOITATION AND ABUSE (TF-CSEA)

Central to the workshop was the in-depth exploration of Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA)—a rapidly evolving form of abuse that takes place entirely or partially through digital means. This discussion sought to clarify misconceptions, define key terms, and equip participants with the analytical tools to understand and confront TF-CSEA effectively.

Participants explored several unique characteristics of TF-CSEA:

- Remote in nature: Abuse can occur without any physical contact, making it difficult to detect or prevent using traditional safeguarding methods.
- Anonymity and reach: Offenders can hide their identities and operate across borders, often exploiting weak regulatory and legal systems.
- Persistent and replicable: Once abuse content is created or shared online, it can be stored, copied, and re-circulated indefinitely.
- Blurring of the lines between digital and physical harm: Online grooming can lead to in-person abuse, or it may exist as a form of standalone psychological and sexual exploitation.

Specific forms of TF-CSEA discussed included:

- **Online Grooming:** Manipulative relationships initiated online, with the goal of sexual exploitation, either through chat, video, or eventual in-person meetings.
- **CSAM (Child Sexual Abuse Material):** The production, distribution, and possession of explicit material involving minors.
- **Sextortion:** The use of threats to force children into producing or sharing sexual content, often starting from seemingly innocuous interactions.

The conversations also touched on the technical challenges of monitoring TF-CSEA:

- Perpetrators using encrypted platforms, VPNs, and dark web forums
- The inability of many national systems to track or remove abusive content
- Platform accountability gaps, where reporting mechanisms are either ineffective or absent

THEMATIC DISCUSSIONS

HIDDEN DIGITAL SPACES AND DIGITAL SAFETY PRACTICES

Understanding the architecture of digital technologies is essential to confronting the evolving threat of technology-facilitated child sexual exploitation and abuse (TF-CSEA). Digital environments are not monolithic; they are layered with each level offering different functionalities, access restrictions, and – critically – levels of in/visibility and accountability/impunity. Any meaningful response to TF-CSEA must begin by recognizing how these layers interact and where they create vulnerabilities.

Through this workshop, participants got to explore the multi-layers of the: **the surface web**, which is indexed and accessible to the general public; **the deep web**, which includes password-protected or unindexed spaces such as private databases and secure communication platforms; and **the dark web**, which is accessible only through specialized software and designed to ensure anonymity. While these spaces were not built with malicious intent, they are often exploited because they lack embedded child safety mechanisms and are difficult to monitor.

This structural understanding of the internet had laid the groundwork for participants to assess and understand how perpetrators exploit its architecture. Abusers typically begin interactions with children on public platforms–social media, messaging apps, gaming networks–where children are easily accessible and content moderation is inconsistent. Once initial contact is made, they often transition to more concealed environments: encrypted messaging services, peer-to-peer networks, or anonymized forums. This migration is neither incidental nor chaotic; it is informed by a strategic reading of platform vulnerabilities, user protections, and the likelihood of detection. Moreover, perpetrators frequently repurpose legitimate technologies for abusive ends, embedding harmful content within harmless formats or using coded language to evade content filters.

This adaptability and technological fluency among perpetrators highlight a critical asymmetry: while abusers exploit digital systems with sophistication, many child protection actors–particularly civil society organizations (CSOs)–remain underprepared to operate securely within the same spaces. Despite their frontline role in safeguarding, CSOs often lack the digital infrastructure and internal policies necessary to protect their operations from technological threats. Workshop discussions revealed that many organizations face serious exposure in several areas:

- **Staff vulnerability,** especially for employees engaged directly with children, who may be targeted for manipulation, coercion, or surveillance;
- **Unsecured communication systems,** which can be infiltrated or spoofed to extract sensitive data or compromise trust;
- **Inadequate cybersecurity practices,** such as the absence of firewalls, unencrypted storage systems, or failure to use two-factor authentication;
- **Limited awareness and digital literacy,** particularly in identifying digital grooming, phishing attempts, or compromised accounts.

In response to these challenges, digital protection must be reframed as a strategic safeguarding priority. Participants in this regard explored a number of safeguarding mechanisms that can help secure their structure's digital use. These include:

- **Technical protections,** such as installing regularly updated firewalls, encrypted communications, and two-factor authentication systems;
- **Policy frameworks,** including internal safeguarding protocols that reflect digital realities and are integrated into broader governance structures;
- **Capacity-building efforts,** ensuring that all staff – regardless of their role – receive training on digital risks, ethical data handling, and secure communication;
- **Clear reporting pathways,** both for internal threats and for external incidents, that would ensure rapid and responsible responses to breaches or abuse.

The Hidden Digital World:
Understanding How Abusers Operate Onlin

THEMATIC DISCUSSIONS

ADVOCACY AND POLICY ENGAGEMENT

The final thematic discussion focused on the role of advocacy in addressing technology-facilitated child sexual exploitation and abuse (TF-CSEA), particularly how civil society can influence public discourse, legal reform, and institutional accountability. It served both as a space for sharing national advocacy strategies and as the starting point for drafting the Recommendation Paper, one of the key outcomes of the workshop.

Key points discussed included:

- **Advocacy as a systemic tool:** Participants emphasized that advocacy should not be limited to raising awareness but should aim to influence policies, shape legal frameworks, and promote accountability.
- **Regional examples of impact:** Participants from five countries shared examples of successful advocacy efforts led by their organizations, illustrating practical ways civil society can drive change.
- **Barriers to effective advocacy:** These included limited government openness to civil society input, lack of media engagement, insufficient data, and low public awareness of TF-CSEA as a distinct issue.

The discussion also introduced several tools and strategies to support advocacy work:

- **Strategic messaging:** Framing TF-CSEA in ways that connect with policymakers, stakeholders, and local communities.
- **Evidence-based approaches:** Using data and survivor testimonies to strengthen the credibility and urgency of advocacy efforts.
- **Regional coordination:** Promoting collaboration across countries to align messaging, share resources, and strengthen collective influence.

FINDINGS AND OBSERVATIONS

Over the course of the three-day workshop, structured exchanges and peer learning activities highlighted a number of persistent and cross-cutting challenges that constrain the effectiveness of efforts to prevent and respond to Technology-Facilitated Child Sexual Exploitation and Abuse (TF-CSEA) across the MENA region. These findings reflect the lived experiences and operational insights of civil society organizations (CSOs) working at the front lines of child protection in some of the region's most under-resourced and complex environments.

In North Africa, TF-CSEA exists within a broader socio-political context shaped by limited institutional reform, regulatory fragmentation, socio-cultural conservatism, and shrinking civic space. These conditions exacerbate protection gaps and reinforce the systemic barriers faced by CSOs, governments, and affected communities. The findings below reflect both structural limitations and regional dynamics that define the current child protection landscape.

Legal loopholes and lack of harmonization

Across the region, existing legal frameworks on child protection and cybercrime often fall short of addressing the specific and evolving nature of TF-CSEA. In many cases, national legislation does not define key offenses such as online grooming, sextortion, or the possession and distribution of child sexual abuse material (CSAM). Even where laws exist, enforcement is inconsistent due to limited institutional capacity, lack of specialization within judicial systems, and weak interagency coordination.

Low technical capacity among frontline professionals

A recurring theme in the workshop was the lack of digital knowledge and preparedness among professionals tasked with child protection. This includes law enforcement officers, educators, social workers, and even CSO staff. Initial knowledge assessments confirmed that many had limited understanding of how digital tools are used to exploit children or how to identify early signs of TF-CSEA.

In a context where digital literacy is uneven and training opportunities are scarce, frontline professionals are often unable to respond effectively or safely. Moreover, state institutions in several North African countries still operate with limited technological infrastructure that further impedes case handling and evidence collection.

FINDINGS AND OBSERVATIONS

Restrictive political environments

In several North African countries, civil society operates under restrictive legal and political frameworks that limit freedom of expression, particularly on sensitive issues such as child sexual abuse. In some contexts, NGOs must navigate laws that tightly regulate advocacy activities or restrict engagement with international actors. This regulatory environment weakens the capacity of CSOs to campaign publicly, engage with government actors, or mobilize broad-based support.

Cultural taboos and silence

Deeply rooted cultural taboos around sexuality, abuse, and honor continue to discourage open discussion of child exploitation. Children who experience TF-CSEA are often unable or unwilling to report abuse due to fear of being blamed, stigmatized, or punished. In conservative communities, these risks are especially acute for girls, who may face reputational harm or family retaliation if they come forward, and for boys who are discouraged from reporting cases of abuse in fear of stigma.

Participants also noted that trust in institutions remains low, particularly among marginalized communities. Many children and their families do not believe that reporting abuse will lead to support or justice which further entrenches cycles of silence.

Lack of reliable data and media engagement

Participants consistently cited the absence of reliable, disaggregated data on TF-CSEA as a key barrier to effective advocacy. Without solid evidence, it is difficult to build compelling narratives or justify policy change. This is further hindered by limited media interest in the issue, which is often sidelined due to social discomfort, editorial constraints, or lack of awareness.

Limited engagement from the private sector

An important structural gap identified by participants is the lack of meaningful engagement from the private sector, particularly technology companies and digital service providers. While these actors play a central role in shaping the online environments where TF-CSEA occurs, their participation in prevention, detection, and response efforts remains minimal across much of the region.

Participants noted that major technology platforms often operate with limited transparency and inconsistent moderation practices, particularly in Arabic-speaking contexts. Reporting mechanisms are frequently inaccessible, slow to respond, or not adapted to the needs of children or local communities. In addition, companies rarely engage with CSOs to develop localized safety features or collaborate on public awareness campaigns.

TOWARD A COORDINATED REGIONAL RESPONSE

RECOMMENDATION PAPER

One of the most significant advocacy milestone of the workshop was the co-creation of the Recommendation Paper—a strategic, action-oriented document intended to serve as a tool for regional advocacy and policy change. The paper offers practical steps for governments, CSOs, and private sector actors to advance child protection online, and represents a unified commitment from workshop participants to lead this charge collectively.

Recommendations for stakeholder: Building & enabling frameworks

Stakeholders are urged to strengthen the legal, institutional, and financial foundations for child online protection:

- **Update legislation:** Enact or revise laws to explicitly address TF-CSEA offenses (e.g. online grooming, sextortion, CSAM), and align them with international standards.
- **Allocate budgets:** Designate specific funding for digital child protection within national child welfare and justice systems.
- **Establish monitoring mechanisms:** Develop local reporting systems and tools for real-time data collection to inform evidence-based policy.
- **Protect whistle-blowers and victims:** Guarantee confidentiality and ensure trauma-informed procedures for survivors and witnesses.
- **Strengthen professional capacity:** Train law enforcement, judiciary, educators, and frontline workers on TF-CSEA detection and response.
- **Institutional accountability:** Regularly evaluate the effectiveness of child protection laws and services, with meaningful civil society and survivor input.

Recommendation for civil society organizations: Strengthening community-level prevention and response

CSOs have a central role in prevention, survivor support, and public engagement. Recommended actions include:

- **Awareness campaigns:** Design targeted, culturally sensitive initiatives for children, caregivers, and educators.
- **Early detection and response:** Train staff to recognize and respond to TF-CSEA, supported by clear internal protocols.
- **Digital safeguarding policies:** Update safeguarding frameworks to include online risks, with regular audits and designated focal points.
- **Survivor services:** Expand access to trauma-informed support (hotlines, legal aid, counseling), particularly for marginalized communities.
- **Child participation:** Create safe channels for children to contribute to policy, program design, and advocacy.
- **Foster a disclosure culture:** Encourage open discussion about digital violence and strengthen mechanisms for safe reporting.
- **Coordination and advocacy:** Build alliances, share data and strategies, and participate in regional networks to scale impact.

Recommendations for the private sector: Ensuring safer digital design and accountability

Technology companies, digital platforms, and service providers are urged to adopt a proactive role in online child protection:

- **Safety-by-Design:** Integrate child protection features–such as privacy settings and content filters–into product development.
- **Monitoring and reporting:** Establish effective systems for detecting and removing harmful content, supported by multilingual reporting tools.
- **Partnership with CSOs:** Co-develop safety tools, share anonymized data, and support awareness efforts through joint initiatives.
- **Digital literacy support:** Sponsor training and integrate educational prompts into platforms used by children.
- **Transparency and oversight:** Publish regular safety reports and undergo independent reviews of content moderation practices.

CONCLUSION

The regional workshop held in Rabat from May 5–7, 2025, marked a pivotal step in the ongoing effort to address technology-facilitated child sexual exploitation and abuse (TF-CSEA) in the MENA region. It convened a diverse group of committed civil society actors to critically examine the risks children face in digital spaces and explore collective strategies for response.

Over three days of dialogue, peer exchange, and collaborative planning, the workshop achieved several key outcomes:

- It deepened shared understanding of TF-CSEA and its manifestations within regional contexts;
- It identified systemic challenges, including legal gaps, limited technical capacity, and inadequate survivor support;
- It amplified the perspectives of those working directly with affected communities;
- And importantly, it initiated the formation of a cross-border coalition centered on advancing children’s digital safety.

At the core of the workshop’s impact is the jointly developed Recommendation Paper. More than a list of policy proposals, it represents a collective commitment to action—grounded in the practical realities of the region and informed by the experiences of those closest to the issue. It outlines concrete steps for governments, civil society, and the private sector to improve online child protection and ensure accountability.

However, as participants emphasized, the workshop is not an endpoint but a starting point. The knowledge, tools, and shared priorities that emerged must now translate into sustained advocacy, regional cooperation, and institutional reform. Moving forward will require:

- Political will to update laws and invest in child-focused services;
- Strategic, cross-sector coordination;
- And an empowered civil society capable of driving change at all levels.

The threats children face online are evolving and transnational. Addressing them requires a response that is equally adaptive, collaborative, and regionally coherent. The Rabat workshop showed that when expertise and shared purpose come together, meaningful progress is possible.

This report, henceforth; stands not only as a record of what was discussed, but as a foundation for the actions that must follow.

ديجي آمن

ⴷⵉⵊⵉ ⴰⵎⵉⵏ

DIGI-AMEN