

HIDDEN IN PLAIN SIGHT

A study of online child sexual exploitation in Pakistan



Fakhruddin G. Ebrahim Fellowship

Hidden in Plain Sight

A study of online child sexual exploitation in Pakistan

Fatima Razzaq

Fakhruddin G. Ebrahim Fellowship



Human Rights Commission of Pakistan

© 2026 Human Rights Commission of Pakistan

All rights reserved. Any part of this publication may be reproduced by duly acknowledging the source.

Every effort has been made to ensure the accuracy of the contents of this publication. The Human Rights Commission of Pakistan takes no responsibility for any unintentional omissions.

Human Rights Commission of Pakistan

Aiwan-e-Jamhooir

107 Tipu Block, New Garden Town

Lahore 54600

T: +92 42 3583 8341, 3586 4994, 3586 9969

E: hrcp@hrcp-web.org

www.hrcp-web.org

Acknowledgements

The Human Rights Commission of Pakistan (HRCP) is grateful to Fatima Razzaq, the organisation's Fakhruddin G. Ebrahim Fellow for 2025, for researching and writing this report. We would like to thank Irfan Khan for editing the document, Farah Zia and Maheen Pracha for reviewing it, Spogmai Rabnawaz for designing the cover illustration, and Maryam Saeed for developing the cover. HRCP is especially grateful to the Ebrahim family for sponsoring the fellowship under which this study was carried out.

Contents

Introduction	1
Methodology	3
Muzaffargarh: Local abuse, transnational demand	4
Anatomy of a ‘fight club’	4
From ‘child pornography’ to OCSEA	6
Grooming, coercion, and digital control	7
OCSEA as a violation of child and digital rights	7
Prevalence and emerging methods of OCSEA in Pakistan.....	9
Emerging forms of OCSEA.....	11
AI-generated and synthetic child sexual abuse material.....	13
Child rights, abuse, and the limits of legal protection in Pakistan	15
Constitutional and legal framework	15
Legislative responses to child abuse.....	15
Evidence handling and secondary harm.....	17
Conclusion.....	20
Recommendations	22

Introduction

According to news reports, in May 2025, the National Cyber Crime Investigation Agency (NCCIA) in Pakistan quietly dismantled one of the country's most disturbing child sexual exploitation networks. The operation in Muzaffargarh district uncovered an international group, led by a German national, that established a so-called 'fight club' to lure, groom, and exploit children aged six to ten.¹ The club, equipped with digital cameras and high-speed internet, provided what officials called 'state-of-the-art facilities' while secretly recording and live-streaming abuse on the dark web to international buyers. Investigators confirmed the footage was sold for thousands of dollars and that at least 50 children were victimised.

When the case was disclosed, the Minister of State for Interior stated that the NCCIA acted on intelligence from the US-based National Center for Missing and Exploited Children (NCMEC). This connection placed a crime originating in rural South Punjab within a broader, transnational network of online child sexual exploitation and abuse (OCSEA).

Two weeks later, another case was reported in Muzaffargarh. A child filed a complaint with Saddar Police Station, alleging sexual abuse and blackmail through online distribution of recorded material.² Within days of the suspect's arrest, three additional children reported similar abuse, stating that videos had been shared on Facebook.

Civil society data highlights the scale of the issue. In its annual report, *Cruel Numbers 2024*, Sahil documented 3,364 reported cases of child abuse nationwide, including sexual abuse, abduction, and child marriage.³ However, these figures reflect only reported incidents. Under-reporting, stigma, and bureaucratic opacity mean most cases, especially those involving online abuse, remain unreported.

Pakistan's digital landscape is expanding rapidly. By October 2025, the country had 117 million internet users and 79.9 million active social media accounts,⁴ many of which were used by children or accessible through shared family devices. Digital rights experts warn that children are exposed to inappropriate content at an unprecedented scale, with risks increasing alongside technological access. Widespread connectivity, weak regulatory oversight, and limited digital literacy have made Pakistani children particularly vulnerable to grooming, blackmail, sexual coercion, and trafficking through online channels.

The restructuring of the Federal Investigation Agency (FIA)'s cybercrime wing into the NCCIA has positioned it as the central institution responding to such offences. The NCCIA now serves as the primary recipient of NCMEC CyberTipline referrals, receiving alerts about accounts, materials, and users linked to OCSEA activity originating in Pakistan. This cooperation raises important questions. Does the NCCIA have the capacity, legal authority, and commitment to

¹ NCCIA busts German-led child sexual exploitation gang in Muzaffargarh. (2025, June 3). *Dawn*.

² M. Ali. (2025, June 20). Suspect arrested as another case of child pornography comes to light in Punjab's Muzaffargarh. *Dawn*.

³ Sahil. (2025). *Cruel numbers 2024: A compilation of statistics on child sexual abuse cases in Pakistan*.

⁴ <https://datareportal.com/reports/digital-2026-pakistan>

pursue these leads effectively? There is no publicly available data on how many NCMEC referrals result in investigations, arrests, or prosecutions. Additionally, there are no statutory requirements for transparency, inter-agency coordination, or victim-centred justice in digital child exploitation cases.

Pakistan is one of the countries most affected by online child exploitation in South Asia. A comparative study found approximately 41.3 cases of child sexual abuse material exposure per 10,000 people in Pakistan, a rate much higher than in India and Nepal.⁵ This situates Pakistan as both a site of victimisation and a node in global systems of demand, production, and circulation operating through largely unregulated digital infrastructures.

These patterns should be viewed through both child rights and digital rights perspectives. Pakistan has ratified the United Nations Convention on the Rights of the Child (UNCRC) and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, committing to protect children from ‘all forms of sexual exploitation and sexual abuse’. However, putting these commitments into practice remains challenging. OCSEA is still not clearly defined as a standalone child rights violation in Pakistan.

There is a limited systematic understanding of how online abuse occurs, how prevalent it is, or how deeply it is embedded in daily digital interactions. Gaps in awareness, research, and institutional training allow the problem to persist largely unnoticed. Law enforcement agencies remain ill-equipped to recognise digital rights violations as child rights violations. Grooming, extortion, and AI-generated sexual imagery are rarely identified early as abuse. Victims and families often must navigate the opaque reporting mechanisms of international technology companies, which are shaped by corporate priorities and distant jurisdictions. Without domestic protocols for swift content removal or psychological support, families experience digital abandonment, with their suffering mediated through platforms rather than justice.

The failure to protect children online is therefore not simply a technological lapse. It is a crisis of governance and rights. OCSEA in Pakistan lies at the intersection of state accountability, technological regulation, and social silence. It is condemned when exposed, then allowed to fade from view.

Given this context, the Human Rights Commission of Pakistan (HRCP) decided to commission a study, using the Muzaffargarh case as an entry point, to examine how Pakistan’s legal, institutional, and social structures address online child sexual exploitation and abuse. The case serves as a diagnostic example because it shows how exploitation can move across physical spaces, online platforms, and transnational networks. Through a child rights and digital rights perspective, the report explores how responsibility is assigned—and avoided—in the digital age. It examines how harm is identified, which institutions respond, what protections exist for children, and where accountability breaks down.

⁵ Childlight. (2025). *2025 Into the light: Index on global child sexual exploitation and abuse*.

Methodology

The study draws on interviews with officials, first-hand accounts, case material, media reports, and analysis of official data. It reviews existing policies and mapping exercises, including the National Commission on the Rights of the Child (NCRC)'s Situation Analysis of Child Online Protection in Pakistan. The study also examines relevant provisions of the Pakistan Penal Code (PPC), the Prevention of Electronic Crimes Act (PECA), provincial child protection laws, and Pakistan's international child rights obligations to understand the legal framework.

The report does not provide a statistical estimate of online child sexual exploitation and abuse in Pakistan, as no national database tracks relevant complaints, investigations, referrals, prosecutions, victim support, or case outcomes. Instead, it analyses available evidence to identify patterns in recognition, response, and institutional failure.

While previous studies offer valuable insights into institutional design and coordination mechanisms, they are necessarily shaped by their positioning. This report takes a different approach by focusing on lived experience, case-based analysis, and questions of accountability. Rather than asking only how child online protection systems are intended to function, it examines how they operate in practice and identifies where children remain unprotected. The study argues that protecting children in Pakistan's digital spaces must be recognised as a core human rights obligation, not a secondary aspect of cybercrime. Until child-protection principles are fully integrated into digital governance, the most vulnerable will remain unprotected—silenced first by fear, and then by neglect.

This research adheres to strict ethical standards. It does not reproduce or describe child sexual abuse material in detail. References to recorded abuse are limited to what is necessary for legal, institutional, and rights-based analysis. The report prioritises the privacy, dignity, and safety of children.

This research is limited by the scarcity of public information on OCSEA in Pakistan. Available official data is fragmented and often lacks breakdowns by age, gender, platform, offence type, investigative outcome, or victim support response. NCMEC CyberTipline referrals and platform transparency figures indicate digital activity related to child sexual abuse material, but do not directly measure victimisation. These figures may include duplicate reports, automated detections, recirculated material, or accounts linked to Pakistan, without confirming where the abuse occurred.

The report recognises that the Muzaffargarh case is still ongoing from both legal and institutional perspectives. Details on prosecutions, evidence handling, international cooperation, and survivor rehabilitation may change as proceedings progress. This analysis should be viewed as an assessment of current evidence and systemic gaps, not as a final determination of criminal liability.

Muzaffargarh: Local abuse, transnational demand

Anatomy of a ‘fight club’

On the night of 23 May 2025, as residents of Adda Bahar, a small settlement roughly 2 km outside Kot Addu, settled into their homes after a day of labour, the quiet was broken by an unfamiliar commotion.⁶ Within minutes, people stepped into narrow lanes, drawn by the sight of police vehicles converging on a modest brick house.

The house belonged to Shafi Khosa, a farmer and daily-wage labourer. Dozens of police vehicles were stationed outside. Few in the gathering crowd understood what was unfolding. Fewer still could have imagined that they were witnessing the exposure of one of the most disturbing cases of online child sexual exploitation and abuse documented in Pakistan.

That night, teams from the NCCIA, the Special Branch, and local police raided the premises. The facility, presented as a small games and fitness centre, was equipped with digital cameras, webcams, professional lighting equipment, and high-speed internet.

Kot Addu, with a population of just over one million, of whom nearly 80 percent live in rural areas, is the main urban centre for surrounding towns and villages. Adda Bahar falls under the jurisdiction of Daira Deen Panah, an area characterised by agricultural work and daily-wage labour, and a lack of organised recreational spaces for children.

According to neighbours, Khosa’s 19-year-old son, Junaid, told residents that he had set up a facility inside the house to teach children physical fitness. Some referred to it as a ‘fighting school’. Adults rarely entered the premises, but children—mostly boys, including relatives and friends—began going there regularly.

One resident noted that children in the area had little to do after school or work. Letting them attend the facility seemed preferable to having them roam the streets. ‘Their own family’s children were going there to play,’ he said. ‘We never thought there was any reason to suspect something wrong.’

What families did not see was how exposed their children were—not only because of economic pressures that left parents away for long hours, but also because of limited understanding of digital technologies and the forms of harm they can enable. Many of the children who entered the facility had little sense of what was being done to them, or how the abuse extended far beyond the walls of the house.

One child, now at the Child Protection Bureau in Multan, described his experience with a calmness that was difficult to hear. At 12, he had never attended school and earned small amounts selling

⁶ This incident was documented by the author, who spoke to residents as part of her research for this study. See also I. Khan & I. Gabol. (2025, June 4). ‘Dark web’ child exploitation ring busted in Muzaffargarh. *Dawn*.

nimko at a local bus stop. One evening, his cousin took him to Khosa's house to watch what he was told would be a 'fight'. He said he was surprised the fight involved naked bodies, but insisted it was 'just a fight'. He repeated the phrase several times, as though reassuring himself. The normality in his tone was striking. Records at the Child Protection Bureau later confirmed he was among the children repeatedly sexually abused and recorded at the facility.

Investigators found that dozens of children were brought to the compound daily. They were coerced into performing sexual acts that were filmed and, in some instances, live-streamed. The footage was sold through encrypted channels on the dark web, generating thousands of dollars. The compound was equipped with professional cameras, high-speed internet, and webcams for real-time transmission.

The NCCIA director general, Waqar Uddin Syed, later described the case at a press conference held in June 2025 as the 'first and only incident of its kind in Pakistan', where a locally operated studio was producing material directly for international dark-web markets. According to him, the material was priced between \$100 and \$500, depending on video quality, length, and specific requirements.

Footage reviewed for the purposes of this study showed rooms lined with green chroma wallpaper, commonly used in professional studios to digitally alter backgrounds. Investigators believe the equipment was sourced and installed by a German national identified as the 'mastermind' behind the network.⁷ The Foreign Office has contacted Interpol for his arrest, and Special Branch sources have confirmed that several local accomplices have been taken into custody.

According to a local reporter, the operation was carried out in strict secrecy. It lasted nearly five hours and involved more than 100 personnel from various law enforcement agencies. Local police were asked to assist without being fully briefed on the nature of the raid. Even after arrests were made, local journalists recount that they were barred from reporting on the case for weeks. The first information report (FIR)—crucial for establishing the legal record—was not shared with the media, even after officials publicly acknowledged the case at a press conference.

Two suspects were arrested at the scene. Ten children, aged 6 to 10, were recovered. Six were placed in the care of the Child Protection Bureau in Multan after authorities determined that returning them to their families was unsafe; investigators believed some relatives had enabled or ignored the abuse. On 2 June 2025, the Minister of State for Interior, Talal Chaudhry, provided details at a press conference in Islamabad, calling the case 'a shocking testament to our moral demise'.

What distinguishes the Muzaffargarh case is not only its scale, but also the way digital tools shaped every stage of the abuse. Children were not abducted; they were invited, persuaded, rewarded, and gradually normalised into a seemingly benign setting. The fight club did not resemble a crime scene. It was designed to look like a place of learning and leisure—a space where children could gather without suspicion.

The pattern was familiar: children were groomed over time, encouraged to return, and gradually coerced into compliance. Recording equipment and internet connectivity were central to the operation. The abuse was designed for circulation. Footage was stored, transmitted, and sometimes live-streamed to buyers abroad. Payment moved through encrypted channels. While the site functioned as a production space, the crime extended far beyond it.

This is why the case cannot be understood as abuse occurring 'offline'. Without digital infrastructure, the operation would not have been possible at this scale or speed. Muzaffargarh is

⁷ Based on the author's interviews with Special Branch officers.

not only a site of abuse, but also an example of how exploitation is increasingly organised around online demand, anonymity, and distribution.

As of this writing, there is limited public information on the status of prosecutions, efforts to locate the foreign suspect, management of seized digital evidence, or the long-term rehabilitation of the children recovered from the site. This lack of transparency is notable and reflects a broader trend in OCSEA cases. While initial enforcement actions may attract public attention, subsequent prosecution, victim support, content removal, and institutional accountability often receive little visibility.

From ‘child pornography’ to OCSEA

In Pakistan, cases such as Muzaffargarh are routinely described as incidents of ‘child pornography’ in media, public discourse, and legal contexts. This term misrepresents the crime, as pornography suggests consent, performance, and consumption—none of which apply to children. Such framing shifts focus from the child to the material, as though the main harm lies in circulation rather than the coercion and violence involved. It also overlooks the acts of grooming, manipulation, threats, and economic exploitation that occur before recording.

Internationally, this terminology is being reconsidered. Child rights organisations now prefer the term ‘online child sexual exploitation and abuse’ (OCSEA) to describe a continuum of harms facilitated or amplified by digital technologies. This shift in terminology is reflected in the Luxembourg Guidelines, developed by a global interagency working group that includes the United Nations Committee on the Rights of the Child and the United Nations Special Rapporteur on the sale of children, child prostitution, and child pornography. The guidelines advise against terms that imply consent or minimise abuse and instead promote language that recognises children as victims of exploitation rather than participants in sexual activity.⁸

OCSEA recognises that abuse does not begin with an image, nor does it end with its removal. It encompasses the full lifecycle of exploitation: initial contact, grooming, recording, circulation, blackmail, and long-term psychological harm. Seen through this lens, the Muzaffargarh case is not exceptional. Digital tools were not accessories to the crime; they were its enablers.

Child sexual abuse material (CSAM) refers to images, videos, or audio recordings documenting the sexual abuse of a child. Unlike ‘child pornography’, it emphasises abuse and recognises such material as evidence of a crime, not illicit entertainment. CSAM should be recognised as both contraband and a record of a child-rights violation. It is not simply content to be removed, but evidence of harm that may require identifying the child, protecting them from further abuse, providing long-term support, and investigating offenders.

CSAM can be produced through physical coercion, emotional manipulation, deception, or economic pressure. It may involve a single incident or repeated abuse. Sometimes, children are forced to perform in front of a camera; in other cases, they are deceived into producing images later used for blackmail. Increasingly, abuse is live-streamed, allowing perpetrators to direct acts remotely in real time.

The material found in Muzaffargarh fits squarely within this definition. The presence of professional recording equipment, the use of live-streaming technologies, and the sale of footage through encrypted platforms point to a deliberate effort to produce CSAM for an international market. The children were not passive subjects of a single recording; they were drawn into a cycle of abuse sustained through threats of exposure and, in some cases, small financial incentives.

⁸ ECPAT International. (2016). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*.

CSAM is uniquely devastating because it produces a lasting record of harm. Even when perpetrators are arrested, the material does not simply disappear. Images and videos may continue to circulate or resurface years later. In contexts such as Pakistan—where access to takedown mechanisms is uneven and specialised psychological support is limited—this permanence deepens the harm.

Pakistani law continues to use terms such as ‘child pornography’ in certain contexts. This report adopts CSAM and OCSEA as analytical and rights-based terms, while acknowledging that legal proceedings may still rely on statutory language. This distinction is important because legal action may address the circulation of material without fully considering the broader exploitation involved.

Grooming, coercion, and digital control

CSAM is rarely produced without grooming. Grooming is not a single act but a process that gradually erodes boundaries and enables abuse. In digital environments, this process is often less visible and more sustained. Children may be contacted through social media, gaming platforms, messaging apps, or informal online spaces. Conversations begin innocuously, trust is gradually built, rewards are offered, and resistance is slowly diminished.

The Muzaffargarh case shows how grooming can move fluidly between physical and digital spaces. Children were brought into a physical environment where trust had already been established. Digital tools then reinforced control. Recordings served as leverage, threats of exposure ensured silence, and online circulation made withdrawal difficult or impossible.

Digital platforms enable perpetrators to remain present in a child’s life without physical proximity. They allow abuse to continue even after a child leaves a particular space. Once material exists, control persists. Grooming, in these contexts, becomes not only a way to initiate abuse, but a mechanism of long-term domination—one that extends well beyond the initial act.

A case in Dera Ismail Khan illustrates grooming and coercion. In November 2024, the FIA Cyber Crime Circle reportedly arrested a suspect who befriended minors on Facebook while posing as a girl. The suspect concealed his identity, groomed the children, and coerced them into inappropriate acts, which he recorded and used to blackmail the victims and their families. Police recovered a mobile device allegedly containing multiple indecent videos of children during the raid.⁹

In Pakistan, grooming is rarely recognised as a standalone harm. It is often dismissed as inappropriate communication or ‘bad influence’ rather than understood as a deliberate strategy of exploitation. This lack of understanding leaves children unprotected at precisely the moment when intervention could prevent more serious abuse.

OCSEA as a violation of child and digital rights

Understanding online child sexual exploitation and abuse requires moving beyond criminal labels and recognising it as a violation of fundamental rights. The UNCRC affirms children’s rights to protection from all forms of sexual exploitation and abuse, as well as their rights to privacy, dignity, and safety. These rights do not stop at the boundary between physical and digital spaces.

The UN Committee on the Rights of the Child clarified this principle in General Comment No. 25, affirming that children’s rights apply fully in online contexts and that states must ensure digital environments protect children’s rights to safety, privacy, participation, information, and

⁹ FIA puts shackles on child pornographer. (2024, November 7). *The Express Tribune*.

remedies.¹⁰ This is especially relevant to OCSEA, as states are required not only to respond to harm but also to prevent digital exploitation, regulate businesses impacting children, and provide child-sensitive remedies for rights violations.

In practice, Pakistan's child protection framework has not fully extended to the digital realm. Laws addressing sexual violence continue to focus largely on physical acts. Cybercrime legislation, where it exists, tends to treat exploitation as a technical or procedural offence rather than a child protection concern. As a result, children harmed online frequently fall outside institutional mandates. This gap became visible repeatedly while working through case material for this research.

OCSEA exposes fragmentation at every level. When abuse occurs online, responsibility is unclear. Law enforcement agencies dispute jurisdiction, platforms defer to internal reporting processes, and families must navigate opaque systems that prioritise content moderation over child welfare. In this environment, rights exist mostly on paper—invoked after harm has occurred, rather than embedded in structures meant to prevent it.

Digital rights sit at the centre of this failure. Children's rights to privacy, data protection, and safety in online spaces are rarely articulated as rights in Pakistani policy. Age safeguards, consent frameworks, and platform protections are largely dictated by global technology companies rather than domestic law. This delegation of responsibility leaves children exposed in spaces that are now central to their everyday social lives.

The reluctance to name and define OCSEA has tangible consequences. When abuse is framed narrowly as 'pornography', responses focus on removing images rather than on the child who has been harmed. When grooming is dismissed as merely inappropriate behaviour, opportunities for early intervention are missed. Treating digital harm as secondary weakens institutional accountability.

The Muzaffargarh case forced a moment of recognition, but such moments are rare. Most OCSEA cases do not reach national attention and remain scattered across police complaints, platform reports, and private conversations. Without a shared framework, they do not coalesce into action.

Recognising OCSEA as a distinct form of violence against children is therefore not an academic exercise. It is a prerequisite for protection, and shapes how laws are written, how institutions coordinate, and how harm is understood. Until this recognition takes root, children will continue to encounter digital spaces not as sites of opportunity, but as largely unregulated spaces of risk.

¹⁰ CRC. *General comment No. 25 (2021) on children's rights in relation to the digital environment*. UN Doc. CRC/C/GC/25, 2 March 2021.

Prevalence and emerging methods of OCSEA in Pakistan

Understanding the prevalence of online child sexual exploitation and abuse in Pakistan is hindered by the lack of a national database tracking cases across provinces, police units, or digital platforms. No institution consolidates complaints, investigations, referrals, and outcomes into a coherent public record. Instead, information is fragmented, relying on media reports, civil society compilations, helpline data, platform detections, and referrals from international intermediaries. Each source indicates scale, but none provides a complete picture.

Civil society monitoring remains the most visible source of information. Sahil's Cruel Numbers 2024 recorded 3,364 reported cases of child abuse across Pakistan in a single year—an average of nine cases per day. Girls comprised 53 percent of victims and boys 47 percent, with Punjab accounting for over three-fourths of all cases. However, these figures are incomplete, as they rely on newspaper reports that only capture publicly disclosed incidents. Abuse that unfolds online—through private messages, closed groups, or encrypted platforms—is far less likely to be reported in the press and often never reaches the police.

Table 1: Reported cases of child abuse in Pakistan (2020–24)

<i>Year</i>	<i>Total reported cases</i>	<i>Girls (%)</i>	<i>Boys (%)</i>	<i>Average cases per day</i>
2020	2,960	56%	44%	8
2021	2,826	52%	48%	8
2022	3,445	54%	46%	9
2023	3,174	51%	49%	9
2024	3,364	53%	47%	9

Source: Sahil.

This issue is not merely one of reporting volume, but of recognition. Many cases involving minors are logged as cyber harassment, online blackmail, or image-based abuse rather than being identified as sexual exploitation. A case from Lahore in August 2025 highlights this issue. The NCCIA's remand application states the accused was arrested following a tip-off from an international organisation and was alleged to have shared pornographic material via Snapchat and engaged in 'sextortion' of a minor.¹¹ However, the FIR was reportedly registered under Section 22 of PECA, which addresses unauthorised use of identity information. This discrepancy is concerning, as it demonstrates how acts described as sextortion of a minor may be recorded as identity-related offences instead of under child sexual exploitation laws.

¹¹ R. Bilal. (2025, August 21). Lahore man accused of 'sextortion' of minor sent on 5-day physical remand. *Dawn*.

It is important to note that grooming and sextortion are rarely detected in their early stages. They surface only when threats escalate, when images begin circulating, or when families discover what has already happened. By that point, the harm is already entrenched. This pattern was observed repeatedly during the review of case materials for this research. The Digital Rights Foundation, which operates a national cyber harassment helpline, has documented similar trends. Survivors often seek help late only when the situation becomes unmanageable. Early warning signs—sexualised conversations, coercive requests, escalating pressure—are frequently dismissed. In cases involving children, the absence of clear procedural categories for sextortion and online grooming means sexual exploitation is frequently misclassified, diluting both the severity of the offence and the institutional response.

In the absence of comprehensive national data, platform-generated reporting has increasingly filled the void. Global technology companies subject to the US law are required to report suspected child sexual abuse material detected on their services to the NCMEC. One of the largest sources of global reporting on online child sexual abuse material is the CyberTipline operated by the NCMEC. In recent years, the CyberTipline has received tens of millions of reports annually from electronic service providers worldwide, reflecting automated detection and platform reporting rather than disclosures by victims or families.

Pakistan frequently appears in referral streams, with reports linked to digital activity from accounts, IP addresses, or material originating in the country. These figures reflect platform-generated reports of suspected child sexual abuse material, but do not directly measure victimisation. They indicate the scale of activity, yet do not reveal how many children were harmed, whether the material was new or recirculated, if the child was in Pakistan, or whether the referral led to investigation, prosecution, or victim support.

Table 2: Number of total reports (including referrals) for Pakistan

<i>Year</i>	<i>Total reports</i>
2020	1,288,513
2021	2,030,801
2022	2,059,884
2023	1,924,739
2024	1,036,608

Source: <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>

The key issue is what occurs after these referrals are received. NCMEC reports mark the start of the protection process. While they identify suspected material, accounts, users, or technical indicators, domestic institutions must assess referrals, preserve evidence, identify children where possible, locate suspects, coordinate with relevant authorities, and determine if urgent protection is needed.

Currently, there is no public data on how many NCMEC referrals to Pakistani authorities result in inquiries, FIRs, arrests, prosecutions, convictions, child identification, content removal, or psychosocial support. This lack of outcome data creates a significant accountability gap and prevents assessment of whether international reporting leads to domestic protection. The gap is especially concerning for time-sensitive OCSEA cases, as delays can allow material to spread, offenders to erase evidence, children to remain in abusive environments, and threats to intensify. A system that receives many international referrals but does not report outcomes risks becoming a passive recipient of information rather than an active child protection mechanism.

Without this crucial link, platform and NCMEC data may create a false sense of visibility. The state may be aware of suspicious digital activity, but the public cannot determine whether children are being identified, protected, or supported. This creates a visibility paradox: harmful material is detected globally, yet the child behind it remains largely unseen within domestic institutions.

Platform actions often end with removal, suspension, or referral. While these measures may reduce immediate visibility, they do not identify the child, ensure local protection, provide psychological support, preserve evidence for prosecution, or prevent the offender from reoffending elsewhere. A takedown is not equivalent to justice. In Pakistan, the absence of a transparent system connecting platform reports to NCCIA action, child protection referrals, prosecution outcomes, or survivor support means platform moderation may become the final response rather than the start of accountability.

Estimates of external prevalence and exposure point in the same direction, while raising similar cautions about interpretation. International comparisons indicate that Pakistan faces high levels of CSAM-linked digital activity. Childlight’s research found over 1 million CSAM-linked instances associated with Pakistan between 2023 and 2024. With 41.3 cases per 10,000 people, Pakistan ranks between Bangladesh and Nepal.¹² However, these figures are often misread. They do not imply that abuse originates domestically in every case. What they do point to is Pakistan’s location within global systems of circulation, redistribution, and consumption.

Table 3: Regional comparison of CSAM exposure rates

Country	CSAM exposure rate (per 10,000 people)
Maldives	94.0
Bangladesh	64.1
Pakistan	41.3
Nepal	19.4
India	15.5

Source: Childlight.

Platforms detect large volumes of harmful material, while domestic systems record comparatively far fewer complaints and even fewer convictions. The gap does not suggest the harm is overstated. Instead, it reflects that different systems address separate aspects of the issue. Platforms detect content, international reporting systems generate referrals, civil society documents fragments, and domestic institutions record only cases that enter formal channels.

Complaint data from NCCIA provides one of the few indicators of domestic response. In 2025, the NCCIA registered 178 FIRs related to child exploitation, arrested 198 suspects, and secured prison sentences of four to ten years for fourteen individuals. These figures indicate some enforcement activity, but do not specify how many cases stemmed from NCMEC referrals, how many children were identified, whether victims received protection or psychosocial support, or if abusive material was removed from circulation.

Emerging forms of OCSEA

As digital technologies advance, online child sexual exploitation adapts accordingly. These are rarely entirely new forms of abuse. More often, they extend familiar patterns—grooming, coercion, recording—into environments that are harder to recognise and regulate. Gaming platforms, live-

¹² Childlight. (2025). *2025 Into the light: Index on global child sexual exploitation and abuse*.

streaming services, and informal chat spaces have become primary environments for grooming. These spaces are widely accessible to children and remain poorly moderated in Pakistan.

Online child sexual exploitation in Pakistan is increasingly shaped by networked environments rather than isolated incidents. Discussion groups, internet forums, and encrypted messaging platforms sit at the centre of this shift. Some operate on open platforms, while many exist as invitation-only groups on encrypted applications, where access is controlled. These spaces enable abuse and allow perpetrators to exchange advice on targeting children, evading detection, and maintaining control. Sexualised discussions involving children are often presented as humour, fantasy, or shared interest. Images and videos are requested, shared, and traded. In some groups, this material functions as proof of participation; in others, it acts as currency.

The Muzaffargarh case illustrates how digital spaces intersect with physical exploitation. Investigators found that Junaid, a central figure, used the Telegram app to coordinate activities and share information related to the abuse. Encrypted channels allowed instructions and material to move beyond the facility, linking the local crime scene to wider networks.

Roshni Helpline, a non-profit organisation that focuses on recovering missing children, informed the NCRC in November 2022 that interviews with several recovered children revealed manipulation by criminals through chat groups such as WhatsApp and Messenger, as well as classified ads websites like Locanto. In one case, a girl was sexually abused and found in a massage parlour, from which she was recovered.¹³

In March 2023, a court in Faisalabad sentenced an individual to two years in prison and fined him PKR 50,000 for sharing child sexual abuse material in WhatsApp groups. The FIA Cyber Crime Circle Faisalabad registered the case under PECA following a complaint reportedly filed by an international organisation. Media reports connected this case to a broader FIA operation in Punjab targeting online grooming through gaming platforms, livestreaming, blackmail, and CSAM distribution.¹⁴

What emerges is a networked form of harm. In several cases examined in this research, abuse was never intended to remain within mainstream digital environments. Material was uploaded, exchanged, or sold through the dark web—a layer of the internet accessed through anonymising networks rather than standard browsers. Unlike open platforms, dark web forums and marketplaces operate without visible moderation. For perpetrators, this infrastructure offers both reach and insulation. Content circulates globally, payments move anonymously, and networks dissolve and reassemble when exposed.

Sextortion has become one of the most frequently reported forms of online abuse involving minors. In many cases, a single image obtained through deception becomes the basis for prolonged coercion. Data from the Digital Rights Foundation shows that once payments are made, threats tend to escalate rather than stop.

The threat of virality often intensifies abuse, as perpetrators use platforms to spread harmful content. In May 2024, the FIA arrested a man who shared explicit images and videos of minors on TikTok, then blackmailed their families for money.¹⁵ Advocate Miqdad Syed, who has worked on child sexual abuse cases, explains that criminals use virality as an additional strategic harm. ‘They use the virality as a threat and weaponise it to blackmail individuals and their families’. He notes that social stigma often heightens this threat, as victims fear widespread exposure.

Live-streamed abuse presents another set of challenges. Real-time formats allow perpetrators and, in some cases, buyers to dictate acts while avoiding stored evidence. For investigators, this

¹³ National Commission on the Rights of the Child. (2024). *Situation analysis of child online protection in Pakistan*.

¹⁴ Court sentences man for sharing child porn. (2023, March 12). *The Express Tribune*.

¹⁵ M. F. Hassan. (2024, May 3). Arrest made in sexual assault case against minor boy. *The Nation*.

complicates attribution and evidence collection. In most cases, the physical setting is disguised as high-speed internet cafés or gaming rooms where children are lured and become potential targets. In August 2022, police in Pirwadhai, Rawalpindi, raided an internet café where pornographic videos were shown to children.¹⁶

Gaming environments often involve real-time player interaction, making these platforms vulnerable to exploitation and abuse, especially when unmonitored. While social media platforms are monitored and restricted, online gaming typically is not. Abuse can include sharing or storing CSAM through in-game content such as chats, avatars, or profile photos, or via the game's cloud or file hosting solutions. Perpetrators may also post URLs to off-platform CSAM, groom children, commit financial sextortion, or live-stream child abuse using integrated or linked platforms.

AI-generated and synthetic child sexual abuse material

Generative AI has introduced new risks to child protection. Synthetic or AI-generated child sexual abuse material can be produced without a camera, physical contact, or the child's awareness. Existing images of children may be manipulated to create sexualised content. 'Nudification' tools and deepfake technologies can target real children, including classmates, neighbours, or those whose images are publicly available online.

This development complicates current legal and institutional frameworks. Traditional definitions of CSAM often assume the material documents an actual incident of abuse, but synthetic material challenges this assumption. The harm remains significant. If the image resembles a real child, it can be used for humiliation, blackmail, grooming, sexual extortion, or social punishment. Even without physical abuse during production, a child's dignity, privacy, and safety may be violated.

Synthetic CSAM also presents investigative challenges. Police must determine whether the material depicts a real child, uses an identifiable child's likeness, was generated from existing photographs, or is part of a pattern of coercion or blackmail. These assessments require technical expertise that standard cybercrime units may lack.

A child-centred response should not treat synthetic abuse as less serious simply because it may not involve physical contact. The key consideration is whether the material sexualises, exploits, humiliates, threatens, or endangers a child. Laws and policies should be updated to address AI-generated, altered, and pseudo-photographic abuse material, while ensuring targeted children receive protection and support.

Structural vulnerabilities amplify these risks. Rapid digital expansion has not been matched by digital literacy or child-focused safety education. Many children access the internet through shared or unsupervised devices. Poverty shapes recruitment, with children from socio-economically vulnerable households targeted through money, gifts, or promises of opportunity, as seen in the Muzaffargarh case. Social stigma continues to suppress disclosure. Institutional capacity to investigate and follow up remains limited, even when reports are made. This raises the question: why does the harm remain largely hidden?

OCSEA in Pakistan is not simply underreported; it is structurally obscured. Harm is filtered by how cases are named, where reports are directed, and who is counted. Platform systems detect content, civil society records fragments, and state institutions respond inconsistently. The gap between harm and recognition allows abuse to persist with little interruption.

This fragmentation is evident in the different pathways by which OCSEA cases enter official or semi-official systems. Each pathway captures only part of the problem. Platform detection may identify abusive material, but not necessarily the child behind it. NCMEC referrals may alert

¹⁶ Two held for showing pornographic videos to kids in Pindi. (2022, August 31). *The Express Tribune*.

Pakistani authorities, but without public outcome data, it is unclear what follows. Direct FIRs depend on families' willingness and ability to report, despite stigma and fear. Child protection units may encounter victims but often lack the digital mandate or technical capacity to address online circulation and evidence.

Table 5 shows that Pakistan lacks a single child-centred reporting pathway for OCSEA. Instead, cases move through disconnected systems that were not designed around the full lifecycle of online exploitation. One system may see the content, another may receive the complaint, another may hold investigative authority, and another may be responsible for child protection. Because these systems are not integrated, no institution can easily track a case from detection to investigation, prosecution, takedown, and survivor support.

This is not only a problem of measurement; it is a failure of prioritisation. So long as online child sexual exploitation is treated primarily as a cybercrime issue rather than a core child rights concern, its true scale will remain hidden. Children will continue to navigate digital spaces where harm is widespread, normalised, and largely unseen.

Table 5: Pathways for OCSEA case reporting in Pakistan

<i>Reporting pathway</i>	<i>Primary actor</i>	<i>Key limitations</i>
Platform detection → NCMEC	Meta, Google, others	Platform-defined harm
NCMEC → NCCIA	US-based intermediary	No outcome transparency
Direct FIRs	Victims / families	Under-reporting, stigma
Child Protection Units	Provincial bodies	Limited digital scope

Source: NCRC Situation Analysis; FIA practice notes.

Child rights, abuse, and the limits of legal protection in Pakistan

Constitutional and legal framework

Child protection in Pakistan is rooted in a constitutional framework where children are viewed primarily as dependents, welfare subjects, or populations requiring protection rather than as autonomous rights-holders. The constitution of Pakistan recognises children as a vulnerable group and includes several relevant provisions. Article 25(3) permits the state to make ‘special provision’ for women and children, and Article 11(3) prohibits employing children under fourteen in hazardous labour. The provisions in Article 37(e)—promotion of social justice, education, and social welfare—express intent but do not establish enforceable rights.

Children are not recognised as individuals with enforceable legal claims. Instead, they are treated as a group in need of care, with protection implied rather than guaranteed. This orientation shaped Pakistan’s initial approach to child welfare. The National Commission for Child Welfare and Development (NCCWD), established in 1979, advised the government on child-related issues. After Pakistan ratified the UNCRC in 1990, the NCCWD coordinated implementation and reporting obligations.

Ratification marked Pakistan’s first comprehensive international commitment to child rights. Article 34 of the UNCRC obliges states to protect children from ‘all forms of sexual exploitation and sexual abuse’. Although the commitment was broad and unambiguous on paper, its implementation remained largely aspirational.

The NCCWD functioned primarily as a coordinating and advisory body with limited enforcement authority. Its mandate focused on policy harmonisation, not intervention or accountability. The National Plan of Action for Children, developed in the 1990s to align national efforts with international obligations, followed a similar path. It articulated goals related to protection, education, and welfare, but did not establish binding legal duties or responsive institutions.

These early frameworks reveal not a lack of concern, but a particular way of understanding child protection. The focus was on welfare planning and policy alignment, rather than enforceable rights. This distinction becomes critical when examining how Pakistan’s legal system later responded to child abuse—and struggled to adapt as abuse shifted to digital spaces.

Legislative responses to child abuse

For much of Pakistan’s history, child sexual abuse was not treated as a distinct legal category. Instead, it was subsumed within the PPC of 1860, a colonial-era statute structured around notions of morality, obscenity, and public decency rather than child protection. Provisions on ‘unnatural offences’ or obscenity were routinely applied to cases involving children, blurring the distinction between consensual adult conduct and sexual violence against minors. This framing offered little

protection to children. It entrenched stigma, discouraged reporting, and centred punishment rather than prevention or support. Abuse was criminalised but not fully understood.

The 2015 Kasur child abuse scandal, involving the sexual abuse and filming of hundreds of children over several years, marked a turning point. The scale of the abuse and the circulation of footage without intervention prompted legislative action. Parliament passed the Criminal Law (Amendment) Act 2016, which introduced child-specific offences into the PPC, expanded definitions of exploitation, and addressed the production and distribution of child sexual abuse material.

This was an important shift. For the first time, children were recognised in criminal law as victims of sexual violence rather than incidental subjects of moral offences. Penalties were increased, and the definition of ‘child’ was brought closer to international standards. However, the reform was largely reactive, responding to public outrage rather than structural gaps. It expanded criminal liability but did not address the treatment of children during investigations, the handling of digital evidence, or victim support through legal processes.

The Zainab Alert, Response and Recovery Act 2020 was enacted after another high-profile case of child abduction and murder. It established mechanisms for reporting missing children, coordinating responses, and issuing nationwide alerts. While significant, its focus remained reactive and largely offline. Online exploitation, grooming, and image-based abuse were not central to its design.

At the provincial level, legislative activity increased after the 18th Constitutional Amendment was passed. Khyber Pakhtunkhwa’s Child Protection and Welfare Act 2010 was among the first to define child abuse comprehensively, including exposure to harmful content. Sindh’s Child Protection Authority Act 2011 and Balochistan’s Child Protection Act 2016 established provincial authorities, shelters, and referral mechanisms. Punjab’s Destitute and Neglected Children Act 2004, and the Restriction on Employment of Children Act 2016, addressed neglect, child labour, and abuse.

These laws, however, were developed independently, rather than in coordination. Definitions of ‘child’ varied, mandates overlapped, and jurisdiction was fragmented. Critically, digital abuse remained marginal or absent. Provincial child protection systems were designed to respond to abandonment, trafficking, and physical harm—not to exploitation facilitated by digital platforms, and transnational networks.

It is important to note that Pakistan does possess a clear criminal law basis for prosecuting cases involving recorded sexual abuse of children, and that this framework is widely relied upon in practice. Most cases examined for this research—including investigations conducted by the FIA Cybercrime Wing and later by the NCCIA—were charged under provisions introduced through the Criminal Law (Amendment) Act 2016. The amendment inserted Sections 292-A and 292-B into the PPC, explicitly criminalising the production, distribution, possession, access to, and facilitation of material depicting the sexual abuse of a child. It also introduced Section 377-A, which for the first time treated sexual abuse of children as a distinct offence, breaking from earlier provisions that framed such acts primarily through obscenity or moral deviance.

Collectively, these sections marked a substantive shift. Recorded abuse was recognised as a serious offence against children, punishable by imprisonment and substantial fines. In practice, these provisions form the backbone of prosecution. Police charge sheets, court records, and media reporting routinely describe such cases as being pursued under the ‘child pornography’ sections of the PPC. From a prosecutorial standpoint, the framework is functional. It establishes culpability, enables arrest, and allows convictions to be sought where child sexual abuse material is recovered.

However, legal sufficiency is not the same as protection. The PPC provisions are content-focused rather than child-centred. They criminalise the existence and circulation of abuse material, but do

not account for the processes involved in its production, such as grooming, coercion, digital blackmail, and prolonged control. Additionally, they lack guidance on handling sensitive digital evidence, preventing secondary circulation during investigations, and providing structured victim protection and rehabilitation.

This limitation helps explain why online abuse continues to be described, both publicly and institutionally, as ‘child pornography’. The law can identify and punish the offence but has not fully reckoned with the digital conditions that enable exploitation or the long-term rights and needs of affected children.

When abuse shifted online, Pakistan responded with cybercrime legislation rather than child protection laws. PECA 2016 was Pakistan’s first comprehensive attempt to regulate digital conduct. Drafted by the Ministry of Information Technology, PECA was primarily shaped by concerns about cybersecurity, data integrity, and national security. Child protection appeared within this framework, but only incidentally. Provisions addressing ‘modesty’ and child sexual abuse material were placed alongside offences such as hacking, identity theft, and cyberterrorism.

Table 6: Legal instruments addressing child sexual abuse and online harm in Pakistan

<i>Law / instrument</i>	<i>Year</i>	<i>Primary scope</i>	<i>Digital coverage</i>
UNCRC (ratified)	1990	Child rights	Indirect
PPC Amendments (292-A/B, 377-A)	2016	Sexual abuse/CSAM	Limited
PECA	2016	Cybercrime	Incidental
JJSA	2018	Juvenile justice	None
Zainab Alert Act	2020	Missing children	None
PECA amendments	2023	Grooming, enticement	Partial

Source: Statutory texts and parliamentary records.

This framing was significant. Cases involving online sexual exploitation of children were routed to the FIA’s Cybercrime Wing, later restructured as the NCCIA. Investigators primarily trained in financial fraud, online harassment, and data breaches were now responsible for responding to child sexual violence, often without child-sensitive protocols, trauma-informed procedures, or coordination with child protection authorities.

Bushra Khaliq, a child protection worker interviewed for this study, described OCSEA cases as ‘falling between systems’. She notes that cybercrime units focus on devices and accounts, while child protection agencies often become involved only after a rescue. Her organisation has handled several such cases, and she finds working with minors particularly challenging due to the system’s limited regard for their rights. She explains, ‘It is difficult to work as it’s hard to convince families to report such crimes because they fear their izzat might get tarnished’. She further adds that when cases do reach the police, their handling is often insensitive and disregards children’s rights, resulting in further trauma for victims.

Evidence handling and secondary harm

OCSEA investigations require law enforcement agencies to handle some of the most sensitive evidence imaginable: images or videos of children being sexually abused. Mishandling such material can itself become a form of secondary victimisation.

PECA is structurally incapable of handling such cases. It criminalised conduct but did not put in place safeguards for victims. The law says little about how sensitive digital evidence should be handled once recovered. It does not mandate confidentiality protocols for images or videos of

abuse. Nor does it establish mechanisms for psychological support or long-term protection for children whose exploitation is recorded, stored, or recirculated.

The reported circulation of footage from the Muzaffargarh case among local journalists, allegedly through a police source, raises serious concerns about evidence handling and secondary victimisation. It shows that digital evidence is often copied unnecessarily, stored without encryption, viewed by officials without a legitimate investigative purpose, shown to journalists, leaked to the public, or discussed in ways that identify the child.

Pakistan's legal framework does not yet provide a detailed statutory protocol for the handling of OCSEA evidence. PECA criminalises certain forms of online conduct, but it does not establish child-specific safeguards for the seizure, storage, viewing, transfer, retention, and destruction of CSAM evidence. Nor does it clearly require that cybercrime investigators coordinate with child protection professionals when recovered material indicates that a child may still be at risk.

These omissions have serious consequences. Investigations routinely seize highly sensitive material, yet law enforcement agencies lack clear guidance on data storage, access, or retention. This absence is especially troubling, given documented police practices. An investigation by Dawn found that, despite guidelines, police frequently record and circulate videos of suspects and accused persons, often posting them online for visibility or personal projection.

In any context, such practices are troubling. In cases involving sexual abuse, they are actively harmful. The limits of enforcement are therefore not simply a question of resources. They are a question of mandate and training. The NCRC notes that the FIA repeatedly acknowledges its officers are primarily trained to deal with fraud, harassment, and financial offences.

Cases of online child sexual exploitation are processed within the same institutional framework despite their distinct evidentiary, psychological, and safeguarding demands. Advocate Miqdad Syed points out that children are often fearful of reporting; their testimonies are vague, and they are easily intimidated by courtrooms and judges. 'Imagine dealing with such a personal crime and then facing the pressure of the court as a 12-year-old', he says. He recounts instances where children are not even addressed in court. Courts sometimes assume their consent and make decisions without considering their needs or wishes.

In its engagement with the NCRC, the FIA has highlighted the absence of specialised, child-sensitive investigation protocols, particularly in cases involving recovered digital material. Issues relating to evidence storage, controlled access to abuse imagery, and coordination with child protection authorities remain unresolved. The NCRC notes that while individual officers may act with care, the system itself lacks standardised procedures designed to minimise secondary harm to victims. These admissions are significant. They indicate that, even when offences are identified and prosecuted, institutional practices have not adapted to recognise OCSEA as a distinct form of violence against children, rather than as a subset of general cybercrime.

Nighat Dad, founder of the Digital Rights Foundation and member of the Meta Oversight Board, has repeatedly pointed to this gap. She notes that Pakistan lacks established protocols for data handling in cases of sexual assault or online exploitation, including those involving children. This results in secondary harm, as victims' abuse may be mishandled by the very institutions tasked with their protection.

A 2022 FIA investigation illustrates both progress and limitations. The prosecution of a dark web-linked child exploitation gang demonstrated institutional capacity to identify organised networks selling videos of minors to international buyers.¹⁷ However, reporting focused largely on arrests

¹⁷ Shehzad, M. (2022, April 1). FIA busts gang involved in minting money through child pornography. *The Express Tribune*.

and confessions, with little attention to victim support, data safeguards, or judicial outcomes. The case showed that the system can act but also highlighted what remains absent.

Conclusion

The Muzaffargarh case highlights a form of harm that often goes unnoticed. It demonstrates that online child sexual exploitation and abuse in Pakistan is not confined to anonymous digital spaces but is influenced by the social and economic conditions children face. Here, the abuse began in a familiar local environment, initially presented as a space for play or training, before progressing through cameras, encrypted platforms, international buyers, and digital markets.

Therefore, OCSEA cannot be fully understood through the narrow categories of pornography, obscenity, or cybercrime. These labels focus on devices, materials, or platforms, often overlooking the child and the exploitation process. In the cases examined, harm extended beyond the creation of images or videos, involving grooming, manipulation, blackmail, threats, and ongoing fear that abusive material may resurface. Digital abuse can persist long after the initial exploitation.

Pakistan's legal framework has made significant progress. Amendments to the penal code address child sexual abuse material and related offences, while cybercrime laws and provincial child protection measures exist. However, these advances have not produced a cohesive protection system. The state has criminalised aspects of abuse but lacks the broader structure needed to prevent OCSEA, enable early identification, ensure sensitive responses, and support children after rescue. As a result, the response remains uneven, reactive, and fragmented despite the presence of laws and institutions.

A major gap is the lack of recognition. OCSEA is still primarily viewed as a cybercrime issue rather than a violation of children's rights. This perspective influences which agency receives complaints, who manages cases, what information is gathered, how evidence is stored, the involvement of child protection bodies, and whether the child is treated as a rights-holder or merely as a witness.

When online exploitation is addressed through systems intended for fraud, harassment, or technical offences, children's specific needs are often neglected. Effective child protection requires more than tracing devices or securing digital evidence; it demands attention to safety, trauma, confidentiality, family context, and the risk of further harm.

The current institutional framework is highly fragmented. Platform reports may identify harmful material, NCMEC referrals may be forwarded to authorities, families may contact police, child protection institutions may intervene after rescue, and courts may hear charges. However, these pathways do not function as a unified protection system.

There is no public system tracking the number of referrals, investigations, identified children, prosecutions, or victims who receive support. While platform detection, NCMEC referrals, direct FIRs, and child protection units contribute, each operates within its own limits. Without a unified public record, understanding the problem's scale or evaluating the response is difficult.

This lack of data is not just a technical issue; it is a governance failure. When online grooming is recorded as inappropriate communication, sextortion as blackmail, CSAM as pornography, and platform referrals move through unclear channels, the true nature and scale of harm remain

hidden. Children often come to the system's attention only after abuse has escalated or gained public notice.

The Muzaffargarh case also shows the limits of a response centred mainly on arrests. While arrests, prosecutions, and international cooperation are essential for accountability, justice for the child cannot end with the detention of the accused. Recorded abuse continues to affect dignity, privacy, safety, and psychological recovery. Abusive material can be copied, traded, re-uploaded, and used for further coercion. In a society with severe stigma around sexual abuse, fear of exposure can affect a child's life long after the incident. A rights-based response must include support for takedown requests, confidential handling of evidence, psychosocial care, family assessment, rehabilitation, and protection from secondary victimisation.

The report shows that technology has outpaced Pakistan's child protection systems. Children now face risks through messaging apps, gaming, live-streaming, encrypted groups, cloud storage, and increasingly, synthetic or AI-generated imagery. Institutions often respond as if abuse is mainly physical, local, and isolated, but OCSEA is networked, repeatable, scalable, and often transnational. A child may be exploited in one location while material is stored, shared, or viewed elsewhere. An effective response must operate across both digital and physical spaces, keeping the child at the centre.

Digital access itself is not the problem. Children have the right to participate in digital life, including learning, communication, play, and access to information. The solution is not exclusion or moral panic, but protection grounded in rights. Digital spaces must be governed to respect children's dignity, privacy, evolving capacities, and vulnerability to exploitation. Safety must be integrated throughout the system, not added only after harm occurs. This includes law, education, platform accountability, policing, prosecution, and child protection services. Each component has a role, but none is effective in isolation.

The central finding of this report is that Pakistan's shortcomings on OCSEA stem not from a lack of laws, but from the absence of an integrated, child-centred system. While the country has criminal provisions, cybercrime institutions, child protection bodies, and international reporting channels, it lacks a coordinated framework that connects these elements in practice. As a result, children are often shifted between mandates, with responsibility dispersed.

Muzaffargarh should not be seen as an isolated incident that briefly shocked the public. It serves as a warning, illustrating the consequences when poverty, social silence, weak digital literacy, inadequate regulation, and institutional fragmentation converge. The case also demonstrates that the state can act when intelligence, pressure, and public attention align.

A serious response to OCSEA must start by accurately naming the harm. Online child sexual exploitation is not just content to be removed or a cyber offence to investigate; it is a violation of rights, dignity, bodily integrity, privacy, and childhood. Until Pakistan's laws, institutions, data systems, and public discourse reflect this reality, children will remain unprotected in digital spaces.

Recommendations

The research report finds that Pakistan's primary challenge is the absence of a unified, child-centred system to address the complex digital and social realities of OCSEA. The following policy recommendations aim to address these gaps:

Recognise OCSEA as a distinct child-rights violation. Federal and provincial authorities should formally use the terms OCSEA and CSAM in laws, policies, police training, media guidance, and child protection practices. The term 'child pornography' should be avoided, as it conceals coercion, abuse, and lack of consent.

Create a national OCSEA coordination framework. A formal mechanism should link the NCCIA, provincial police, child protection bureaus, NCRC, prosecutors, courts, social welfare and education departments, and relevant civil society organisations. This mechanism must clearly define roles from the initial report through long-term rehabilitation.

Publish anonymised referral and outcome data. The NCCIA should publish aggregate data on NCMEC referrals, domestic complaints, investigations, arrests, prosecutions, convictions, children identified, and victims referred to support services. All data must be anonymised to protect children and ongoing investigations.

Establish child-sensitive investigation protocols. Trained officers should handle OCSEA cases using trauma-informed procedures. Children should not be interviewed repeatedly by different agencies. Interviews must take place in child-friendly spaces, with psychosocial support provided from the outset.

Adopt strict digital evidence safeguards. CSAM evidence should be stored securely, accessed only by authorised personnel, and protected with audit trails. Unnecessary copying, informal viewing, media circulation, or disclosure of identifying details must be strictly prohibited and penalised.

Create a rapid takedown and survivor-support pathway. Children and families should have access to a domestic mechanism for reporting and removing abuse material from platforms. This should connect to global tools and hotlines as needed, but families should not be left to navigate foreign platform systems on their own.

Update law for grooming, sextortion, live-streaming, and synthetic CSAM. Existing criminal law should be reviewed to ensure it addresses online grooming, coercive solicitation, sextortion, live-streamed abuse, AI-generated sexual imagery of children, and possession or facilitation of abuse material on encrypted and cloud-based systems.

Train prosecutors and judges. OCSEA prosecutions require knowledge of digital evidence, grooming dynamics, child testimony, trauma, and the ongoing harm caused by circulation. Specialised training in these areas should be mandatory.

Integrate digital safety into child protection and education. Digital literacy should not be limited to warnings about 'inappropriate content'. Children should be taught how grooming,

coercion, blackmail, privacy violations, and platform manipulation work. Parents, teachers, and community workers should be trained to recognise early warning signs.

Provide long-term rehabilitation. Victim support should include emergency protection, counselling, family assessment, school reintegration, legal aid, privacy protection, and monitoring for retaliation or renewed blackmail. Rehabilitation should continue beyond FIR registration or suspect arrest.