NATIONAL COMMISSION ON
THE RIGHTS OF CHILD

Situation Analysis of Child Online Protection in Pakistan

National Commission on the Rights of Child (NCRC) is an independent statutory body established by the Government of Pakistan for the promotion, protection, and fulfilment of children's rights in Pakistan. NCRC has the mandate to examine and review policies, laws, practices, and proposals, inquire into violations of child rights, conduct research, raise awareness, build capacities, provide technical support, and advise the Government on legislative and policy matters by virtue of the National Commission on the Rights of Child Act, 2017.

Technical Support PTA and UNICEF

PTA

Financial Support UNICEF

unicef
for every child

Designed by **HUMAN** Design Studios

Foreword

The use of the internet and technology is today's reality. New technologies are fundamentally changing the lives of children in the twenty-first century. Children are among the most frequent users of digital spaces; while this presents unprecedented opportunities for learning, creativity, and connection, it also exacerbates the risks of online abuse and exploitation.

The protection of children in the digital sphere transcends geographical boundaries and is a paramount concern on a global level. The internet knows no borders, and as such, the threats posed to children online are not confined to any single nation or region. Pakistan ranks as the 8th largest population of internet users globally and internet penetration continues to rise; and thus, the need to protect children from online threats has never been more pressing.

Children, unfortunately, are exposed to a myriad of dangers in the digital realm and are vulnerable to cyberbullying, online grooming, sharing of sexual abuse materials and Online Child Sexual Exploitation and Abuse (OCSEA) that requires an immediate, multi-sectoral and global response. OCSEA refers to a variety of sexually exploitative and harmful behaviours that take place or are facilitated online and through the use of information technologies.

Child Online Protection (COP) refers to the measures and steps needed to protect children from harm and exploitation through the use of these information technologies. The Government of Pakistan in 2023 has taken significant steps to improve the legislative framework for protecting children online. The Criminal Law Amendments of 2023 represent a comprehensive effort to address gaps in the landscape of online threats to children. These amendments reflect the government's commitment to the safety and well-being of children in the digital sphere. However, the real challenge lies in effectively implementing these changes in both letter and spirit.

COP has been identified as a priority area in the NCRC's Strategic Plan for 2024-2026. The Situation Analysis of Child Online Protection in Pakistan is a comprehensive effort to address the complex issues surrounding the online safety

of children. It delves into the emerging risks posed by the use of the internet by children. Through careful analysis and examination of these risks, the report outlines recommendations to counter OCSEA which includes raising awareness among policymakers, law enforcement agencies, educators, and parents about the urgent need for action.

As Chairperson of the National Commission on the Rights of Child (NCRC), I sincerely appreciate all stakeholders who have played a pivotal role in shaping this report. I extend special thanks to the former Chairperson of the NCRC, Ms. Afshan Tehseen, for initiating the work on this report during her tenure and Mr. Qindeel Shujaat for authoring it. I would also like to thank the Federal Investigation Agency (FIA), Pakistan Telecommunication Authority (PTA) and UNICEF for their important contribution and co-operation in the development of this report.

I urge policymakers, law enforcement agencies, educators, and parents to heed the recommendations put forth in this document. Let us work together to create a safer and more secure online environment for our children.

Ayesha Raza Farooq,
Chairperson,
National Commission on the Rights of Child.

Table of Contents

Acronyms

C3P	Canadian Centre for Child Protection
CAS	Cyber Alert Service
CCRC	Cyber Crime Reporting Centres
CCW	Cyber Crime Wing
CDD	Centre for Digital Democracy
CEOP	Child Exploitation and Online Protection Centre
CGPC	Cyber Governance Policy Committee
COP	Child Online Protection
CRC	Convention on the Rights of the Child
Cr.P.C	Code of Criminal Procedure
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
CSEA	Child Sexual Exploitation and Abuse
CSE	Child Sexual Exploitation
ESP	Electronic Service Provider
FIA	Federal Investigation Agency
FIR	First Information Report
GB	Gilgit-Baltistan
ICMEC	International Centre for Missing and Exploited Children
ICT	Information and Communication Technologies
ICT	Islamabad Capital Territory
ILO	International Labour Organization
INGO	International Non-Governmental Organisation
IOT	Internet Of Things
ISP	Internet Service Provider
ITU	International Telecommunication Union

GC	General Comment
GSMA	Global System for Mobile Communications Association
KP	Khyber Pakhtunkhwa
MNR	Model National Response
MoFEPT	Ministry of Federal Education and Professional Training
MoITT	Ministry of Information Technology and Telecommunications
NCMEC	National Centre for Missing & Exploited Children
NCC	National Curriculum Council
NCRC	National Commission on the Rights of Child
NGO	Non-Governmental Organisation
NHRI	National Human Rights Institution
OCSEA	Online Child Sexual Exploitation and Abuse
OECD	Organisation for Economic Co-operation and Development
OPCP	Optional Protocol on a Communications Procedure
OPSC	Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
PDNCA	Punjab Destitute and Neglected Children Act
PECA	Prevention of Electronic Crime Act
PPA	Pakistan Penal Code
PTA	Pakistan Telecommunication Authority
SCPA	Sindh Child Protection Authority
SDGs	Sustainable Development Goals
TWG	Technical Working Group
UNICEF	United Nations Children's Fund
UCOCA	Unit Counter on Online Child Abuse
XR	Extended Reality

Members NCRC

Ayesha Raza Farooq
Chairperson

Khalid Latif
Secretary NCRC

Khalid Naeem
Member ICT

Mehek Naeem
Member Punjab

Pirbhu Lal Satyani
Member Sindh/Minorities

Nadia Bibi
Member
Khyber Pakhtunkhwa

Muhammad Hassan
Male Child Member

Rabia Imran
Female Child Member

Context

Pakistan is the 8th largest population of internet users in the world (PTA 2022). At the start of 2022, internet penetration in Pakistan stood at 36.5% of the total population, i.e. 82.90 million internet users with 71.70 million active social media users[1].There were increase of 22 million (35.9%) internet users in Pakistan between 2021 and 2022[2]. Data from GSMA Intelligence shows that there were 186.9 million cellular mobile connections in Pakistan at the start of 2022.

The rise of information and communication technologies (ICT), including the internet, has opened up many positive opportunities for adults and children around the world. They can share materials and experiences in unprecedented ways and transcend the physical, geographical, and temporal boundaries of human interaction. The increasing access to internet, mobile technology, and the growing number of internet-enabled devices - combined with the immense resources found in cyberspace - provide unprecedented opportunities for learning, sharing and communicating.

Nowadays, many children have access to a mobile phone, video games and the internet. Although the technology offers tremendous benefits as explained above, children can also face a number of risks. Children may be exposed to inappropriate content for their age or inappropriate contacts, which makes children highly vulnerable to violence including sexual abuse and exploitation - a risk that is growing exponentially with the rapidly increasing use of technology[3]. The internet's new audio and video facilities also provides online predators with a various ways to target, reach out to, exploit and abuse children.

Categories of Risks[4]

According to the OECD typology of risks, there are four emerging risk categories to which parents, educators and children should be alert.

Content risks: These include hateful, harmful, or illegal content and disinformation.

Conduct risks: These refer to children's own behaviour and conduct that can make them vulnerable to exploitation and abuse, e.g. in the case of sexting or cyberbullying.

Contact risks: These include online predators, sex trafficking and cyber-grooming, which are a growing problem in all countries.

Consumer risks: such as inappropriate marketing messages and online fraud.

Overarching Risks

The typology also recognises risks that cut across all risk categories and are seen as highly problematic, as they can significantly affect children's lives in a variety of ways.

Privacy risks: Many children do not yet understand what privacy information they are receiving and the value of their personal data.

Advanced Technologies Risks: The use of AI-based technologies, the Internet of Things (IoT) and extended virtual reality (XR) pose further risks. The immersive virtual worlds within the metaverse bring new and increased threats, many of which are not yet well understood.

Health and wellbeing risks: The potential negative impact of the digital environment on children's health and well-being has caused great public concern and has yet to be further studied to inform adequate law and policy reform, as well as gender-sensitive and child-centric programming.

4 OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en.

These developments have raised legitimate concerns about the danger posed by easy availability of explicit content, online child sexual exploitation and abuse, the associated challenges in detecting and dealing with online perpetrators and, most importantly, the task of identifying and supporting children at risk and affected children. The situation is further complicated by limited awareness and gender biased social norms.

Recent incidents of technology-facilitated violence against children have highlighted the need for efforts to protect children from cyber crimes. However, knowledge and understanding of this issue is limited partly due to the ever-evolving nature of technology. It is also important to analyse the issue not only through the legal framework but also through the technological means.

> The "Kasur child sexual abuse scandal" refers to a series of cases of sexual exploitation and abuse of children that took place between 2006 and 2014 in Kasur district in the province of Punjab, culminating in a major political scandal in 2015[5]. Both media and government officials have described it as the biggest child abuse scandal in Pakistan's history. After the discovery of hundreds of video clips showing children engaged in sexual acts, various Pakistani media estimated that 280 to 300 children, most of them male, had been sexually exploited and abused. The scandal allegedly involved an organised crime ring that sold child sexual abuse material to porn sites while blackmailing and extorting the victims' relatives[6].

The Situation Analysis aims to provide an overview of the current ecosystem of COP in Pakistan and inform legislators, government agencies, law enforcement, development and child protection practitioners about the key issues and gaps posed by ICT that contribute to OCSEA. The report discusses the international legal framework and the law in practice and makes a series of recommendations to key stakeholders on how to protect children from the dangers of ICT.

5 Aliyah, Ali. "Kasur Child Sexual Abuse Case." Pakistan Journal of Applied Social Sciences, Mar. 2020, https://doi.org/10.46568/pjass.v2i1.288.

6 ibid

Different Forms of Online Child Sexual Exploitation and Abuse (OCSEA)

Article 19 of the UN Convention on the Rights of the Child (CRC) defines violence against children as all forms of physical or mental violence, injuries, abuse, neglect, negligent treatment, maltreatment or exploitation, including sexual abuse. Violence can be perpetrated by different people and take place in different settings.

Child Sexual Abuse (CSA)[7] means forcing or enticing a child to engage in sexual activity, whether the child is aware of it or not. This may include activities such as involving children in viewing or producing sexual images, watching sexual activity, encouraging children to behave in sexually inappropriate behaviour, or grooming a child in preparation for abuse.

Child Sexual Exploitation (CSE)[8] is a form of child sexual abuse. It occurs when an individual or group uses a power imbalance to coerce, manipulate, or deceive a child or young person under the age of 18 into sexual activity in exchange for something the victim needs or wants, and/or for the financial gain or status gain of the perpetrator or facilitator. The victim may have been sexually exploited even if the activity appears to be consensual.

Child sexual abuse and exploitation takes on an online dimension when any form of online technology such as the internet is used to produce and share child sexual abuse material. For example, when sexual acts are photographed or video/audio recorded, which are then uploaded and shared online, either for personal use or to share with others.

Online Child Sexual Exploitation and Abuse (OCSEA)

As the internet and sophisticated digital tools have increased, so has the emergence of child sexual exploitation material become accessible online. Images and videos of children can be seen on many internet platforms, such as social media, file sharing services, image sharing websites, webcam video games and even mobile apps[9]. Additionally, people who commit these crimes may join

7 "What Is Online Child Sexual Abuse and Exploitation?" https://www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/. Accessed 10Nov. 2022.

8 Ibid.

9 "Child Pornography." Child Pornography, 26 May 2015, www.justice.gov/criminal-ceos/child-pornography.

internet discussion forums and networks to express their desires and experiences of exploitation of minors and to buy, share or exchange photos.

Online child sexual exploitation and abuse (OCSEA) encompasses a wide range of forms and behaviours. The term OCSEA is used in this report to cover all types of offences. These may include:

Child sexual abuse material[10] refers to material depicting sexual abuse acts of any kind, a child engaged in real or simulated explicit sexual activity, or any depiction of a child's private parts for predominantly sexual purposes or use of children in pornographic performances and materials.

"Child Pornography" does not accurately depict Online Child Sexual Exploitation and Abuse [11]

The term "child pornography" is now commonly referred to as "child sexual abuse material" (CSAM). The term "pornography" suggests that the material is created and distributed for the purpose of sexual gratification, which is not an accurate or adequate characterisation of the harm done to children who are subjected to sexual abuse and exploitation. The use of the term "child sexual abuse material' emphasises the seriousness of the crime and the harm caused to child victims and helps to promote public understanding of the issue. *The Committee on the Rights of the Child recommends that States' parties, in line with recent developments, avoid the term 'child pornography' to the extent possible and use other terms such as the 'use of children in pornographic performances and materials', 'child sexual abuse material' and 'child sexual exploitation material'.*

10 "Glossary of Terms - International Centre for Missing and Exploited Children." Glossary of Terms - International Centre for Missing & Exploited Children, www.icmec.org/resources/glossary. Accessed 27 Dec. 2022.

11 Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography adopted by the Committee at its eighty-first session (13–31 May 2019).

The term "child sexual abuse material" (CSAM) is used in this report, as recommended by the Committee on the Rights of the Child, but the term "child pornography" is used in this document when that term is used by the law.

Cyberbullying[12] occurs when someone, usually a stranger, deliberately and repeatedly harasses another person online by sending them hurtful messages or images or posting negative things about them on websites. This is common on social media platforms such as Facebook, Twitter, and Instagram.

Sexting[13] is sending and receiving sexual messages via technology such as a phone, app, email or webcam. Sexting can include words, photos or videos, such as: a sexually explicit message or post, nude or semi-nude photos/videos, photos/videos of sexual acts, live webcam chats with someone involving sexual acts, photos/videos taken with a webcam, etc.

Sextortion/ sexual extortion[14] is the blackmailing of an adult or child using (self-made) images of that person to extort sexual favours, money or other benefits from them, under the threat of sharing the material without the consent of the person depicted (e.g. posting images on social media or sending them to family members).

Livestreaming of child sexual abuse and exploitation[15] means that children committing or viewing sexual acts or indecent images of children with other perpetrators are broadcast live over the internet (via webcam) to viewers. This happens in online chat rooms, on social media platforms and in communication apps with video chat functions. Livestreaming child sexual abuse viewers can be passive (paid) or active, communicating with the child, the sex offender and/or the facilitator of the sexual abuse and demanding certain physical acts. Another type of livestreaming could involve forcing a child to produce and broadcast sexual content in real time.

Grooming a child for sexual purposes[16] is shorthand for soliciting children for sexual purposes and refers to the process of establishing a relationship with a child in person or through the internet or other digital technologies with the intention of engaging in sexual acts or producing child sexual abuse material.

Both girls and boys can fall into more than one category, and this overlap of risk factors puts them at greater risk of sexual abuse and exploitation.

12 "Cyberbullying." Cyberbullying - National Bullying Prevention Center, www.pacer.org/bullying/info/cyberbullying. Accessed 27 Dec. 2022.

New Technologies and Trends

There are new technologies and new trends that further endanger the lives of children, such as virtual games, deepfake technology and private browsers. Deepfake, for example, is a new trend in OCSEA where perpetrators manipulate photos and videos of children into sexual images in order to extort more sexual images from them[17]. This manipulation can include anything from a photo of a child naked in a swimming costume to showing a child's face on a person's body performing a sex act. The perpetrator then shows the edited images to the victim and threatens to share them with parents, friends, class fellows, or social media if the child does not send him more, often increasingly graphic, photos or videos[18]. Sometimes the perpetrators force the child to extend the abuse to friends or younger siblings, or they invite other perpetrators to join in the sextortion and demand specific or images.

Furthermore, apps and websites that use artificial intelligence to undress children in photos are on the rise. These are popularly referred to as "Nude Generator Technologies" or "Nudify Apps" or "Declothing Apps". "Nude Generator Technologies" use software and algorithms to manipulate images. They use techniques such as deep learning and AI to generate realistic-looking nude photos and explicit content, or either soliciting images from victims via their social media and then edit them to create nude photos with the intention of harassing or blackmailing them, etc[19]. Additionally, users of artistic AI platforms have reportedly created explicit/shocking content with additional features such as features like text-to-image models[20]. Once these images are shared, victims face problems as the manipulated content keeps resurfacing and it is not easy to detect deepfakes with the naked eye. According to the report, these apps are promoted on social media platforms, gaining more and more users, and increasing the vulnerability of minors.

17 "INHOPE | What Is a Deepfake?" INHOPE | What Is a Deepfake?, inhope.org/EN/articles/what-is-a-deepfake. Accessed 15 Nov. 2022.

18 "Teen Boys Increasingly Targeted in Sextortion Schemes, FBI Memphis Says." Teen Boys Increasingly Targeted in Sextortion Schemes, FBI Memphis Says, news.yahoo.com/teen-boys-increasingly-targeted-sextortion-103554698.html. Accessed 15 Dec. 2022.

19 Bloomberg, M. M. (2023, December 9). *'Nudify' Apps That Use AI to 'Undress' Women in Photos Are Soaring in Popularity*. TIME. https://time.com/6344068/nudify-apps-undress-photos-women-artificial-intelligence/

20 Growcoot, M. (2023, December 11). *AI Image Generator Dropped by Computing Provider Over Nonconsensual Nude Pictures*. PetaPixel. https://petapixel.com/2023/12/11/ai-image-generator-dropped-by-computing-provider-over-nonconsensual-nude-pictures/

In 2022, a BBC News investigation discovered that the Metaverse exposes children to "wholly inappropriate" and "incredibly harmful" sexual content[21]. Two journalists investigating VRChat, one of the most popular apps on the Metaverse Oculus Quest shop, have extensively documented sexual harassment of children and their exposure to inappropriate content on virtual platforms[22]. Jess Sherwood, a BBC researcher, pretended to be a 13-year-old girl while exploring virtual spaces in VRChat. She discovered and visited a virtual strip club as part of her investigation, where she witnessed adult men chasing a child and ordering her to undress. Condoms and sex toys were on display in many of the rooms Sherwood entered. She even witnessed a group of adult men and teenagers engaging in group sex on one occasion. She also observed several cases of grooming during her investigation. Journalist Yinka Bokinni made similar observations while investigating for Channel 4 Dispatches as a 22-year-old woman and a 13-year-old child[23]. She was confronted with racist, sexist, and other discriminatory comments from other users within seconds of entering one of VRChat's virtual spaces.

21 *"Metaverse App Allows Kids Into Virtual Strip Clubs." BBC News, www.bbc.com/news/technology-60415317. Accessed 15 Nov. 2022.*

22 *GAMING AND THE METAVERSE*. Bracket Foundation, Value for Good, 2022.

23 ibid

Online Child Sexual Exploitation and Abuse in Pakistan

Sahil, a non-governmental organisation that works against child sexual abuse, reports 145 cases (3.76%) in 2021 and 109 cases (2.56%) in 2022 of OCSEA[24]. In 2021, the Digital Rights Foundation's Cyber Harassment Helpline received 4441 new cases[25]. Children were targeted in 184 cases (4%)[26]. The helpline found that females are generally more vulnerable to extortion and non-consensual use of their information, including but not limited to their pictures, videos, and phone numbers. However, fake profiles and hacked accounts are more likely to have a negative emotional impact on women and damage their reputation in society[27]. This is one of the reasons why few cases are reported to law enforcement in Pakistan.

Roshni Helpline is a non-profit organisation that specialises in recovering missing children and reuniting them with their families. The Roshni team informed the NCRC in November 2022 that while interviewing a number of children after their recovery, they found that some of the children were provoked and manipulated by criminals through chat groups (such as Whatsapp and Messenger) and classified ads websites such as (Locanto). In one case, a girl was sexually abused and ended up in a massage parlour from where she was recovered.

Because the internet knows no borders, cybercrimes are committed in numerous jurisdictions. The users, facilitators and victims can all be in different countries. Most of the popular social media companies are registered in the United States and have users from all over the world, including Pakistan. The National Centre for Missing & Exploited Children's (NCMEC) CyberTipline is the United States' central reporting system for online child exploitation, including child sexual abuse material, child trafficking and online enticement[28]. Because these companies have users around the world and these incidents are reported to NCMEC, the CyberTipline serves as a global clearinghouse.

Companies in the United States must comply with 18 USC 2258A[29], which requires US companies to report to the NCMEC CyberTipline when they become aware of suspected child sexual abuse material on their platforms and servers[30]. The CyberTipline provides the public and online electronic service providers with an easy way to quickly report suspected cases of OCSEA.

The CyberTipline receives cases about various forms of OCSEA on the internet. The number of reports in 2022 has increased in almost every category compared

30 Ibid.

to 2020 and 2019[31]. **Reports of child sexual abuse material (CSAM) make up the largest reporting category. Over 99% of reports received in 2021 and 2022 by the CyberTipline involved incidents of suspected CSAM[32].**

Reports	2019	2020	2021	2022
CSAM (possession, manufacture, and distribution)	16,939,877	21,669,264	29,309,106	31,901,234

Source: CyberTipline

The CyberTipline received more than 29.3 million reports in 2021 and 31 million reports in 2022[33]. Of the total reports, 99% of these reports came from Electronic Service Providers (ESP) reporting cases of apparent child sexual abuse material that they learned about on their systems.

31 "CyberTipline Data." National Center for Missing & Exploited Children, www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.html. Accessed 20 Nov. 2022.

32 ibid.

33 Ibid.

Electronic Service Providers		
	2021	**2022**
Facebook	22,118,952	21,165,208
Google	875,783	2,174,548
Instagram	3,393,654	5,007,902
Microsoft	78,603	108,597
Snapchat	512,522	551,086
Omegle	46,924	608601
WhatsApp	1,372,696	1,017,555
Tiktok	154,618	288,125
Twitter	86,666	98,050
Others	718,207	342,146
Total	29,358,625	31,361,818

Source: CyberTipline

According to NCMEC, the online enticement category saw an 82% increase from 2021 to 2022. One of the factors contributing to this growth was an alarming increase in reports of financial sextortion, a crime in which children are tricked into sharing explicit photos and then threatened by offenders that they will share the images with the child's friends, family or others if they do not give money to the extortionist. Several of these cases have had a tragic outcome as the children have taken their own lives in panic. In previous years, sextortion offenders were more likely to target young girls in order to obtain more explicit images. In 2022, NCMEC report a sharp increase in boys being blackmailed for money rather than images.

Of the cases reported in 2021, most came from India, followed by Philippines and Pakistan, while in 2022 it was India, the Philippines, followed by Bangladesh and then Pakistan[34]. These figures are not representative of the extent of child sexual abuse in any particular country. However, they do indicate that a large amount of content related to child sexual material is consumed, uploaded and distributed from Pakistan. According to the FIA[35], 70% of child sexual abuse material uploaded from Pakistan is non-Asian content produced abroad and re-uploaded and distributed by Pakistani users.

Country	No. of Cases Reported (2021)	No. of Cases Reported (2022)
India	4,699,515	5,675,324
Philippines	3,188,793	2,576,182
Pakistan	2,030,801	2,059,884
Indonesia	1,861,135	1,878,011
Bangladesh	1,743,240	2,145,098
Iraq	1,220,470	905,883
Algeria	1,171,653	731,167

Source: CyberTipline

Although the scale of the problem can be hinted by the statistics from ESPs, there is probably no way of estimating the actual number of victims, as not all content is detected by ESPs. Nonetheless, the available data clearly suggests that there are many more unidentified victims of OCSEA than those who have been identified or have reported complaints to law enforcement. In contrast, only 570 local cases reported to the FIA in three years according to FIA, 113 cases in year 2021, 187 cases in year 2022 and 250 cases in year 2023[36].

34 Country specific numbers may be impacted by the use of proxies and anonymizers.

35 Meeting with Mr. Imran Haider, Cyber Crime Wing, Federal Investigation Agency (FIA), held on December 13, 2022 in Islamabad

36 Information provided by the Federal Investigation Agency (FIA) under Letter No. HQ/FIA/CCW/ISB/CCRC/2023/10226-28, received by the NCRC on January 24, 2024

Pakistan	
Year	**Local Complaints**
2021	133
2022	187
2023	250

Source: FIA

Once the complaint has been received by the FIA, it is examined and, after an initial investigation, a charge is filed. In 2021, the FIA registered 53 FIRs, in 2022 the FIA registered 65 and in 2023 51 FIRs were registered. According to the FIA, 6 convictions were made under registered FIRs in 2023[37].

FIRs Registered on OCSEA for Year 2022 and 2023 (Pakistan)				
Cyber Crime Reporting Centre (CCRC)	**Local Complaints**	**CyberTipline Reports**	**Interpol/ Embassies**	**Total FIRs**
	FIRs Registered on Local Complaint having Section 22 of PECA	FIRs Registered on CyberTipline Reports having Section 22 of PECA	FIRs Registered on Embassies/ Interpol Reports having Section 22 of PECA	
Total (2022)	**25**	**36**	**4**	**65**
Total (2023)	**32**	**17**	**2**	**51**

Source: FIA

37 Information provided by the Federal Investigation Agency (FIA) under Letter No. HQ/FIA/CCW/ISB/CCRC/2023/10226-28, received by the NCRC on January 24, 2024

FIA busted a gang dealing in child sexual abuse material[38]

In April 2022, a gang allegedly making money by sexually abusing children on the dark web was busted in Lahore. At least 10 victims were sexually exploited, according to the initial investigation by the Cybercrime Cell of the Federal Investigations Agency (FIA). The perpetrators, who live in a private residential society in an outskirt of Lahore, lured a child with money or other means, raped him and filmed the entire incident. Afterwards, the perpetrators blackmailed the child into giving them money and repeatedly forced him into sexual exploitation. When he resisted, the perpetrators threatened to publish his video on the internet.

The perpetrators also made money by selling these explicit videos on the dark web. The gang consisted of four members, including one woman. The FIA's Cyber Wing was alerted after the organisation received a complaint about child sexual abuse material. The FIA initiated investigation after receiving the complaint and a large quantity of videos containing child sexual abuse material was recovered from the gang member mobile phone. There were several child victims. According to the information, the gang member lured children by offering them money and valuable gifts and recording their videos, which were then uploaded on the dark web to earn money.

The Cybercrime Cell of the FIA has registered a case against the accused under Sections 20, 21 and 22 of the Prevention of Electronic Crime Act (PECA) 2016 and Section 109 of the Pakistan Penal Code (PPC).

Data released by the Internet Watch Foundation[39] shows that 97% of all child sexual abuse material identified globally in 2021 involved the sexual abuse of girls, compared to only 65% of images seen by analysts ten years ago[40]. Although both

38 "Gang Involved in Child Pornography Busted | the Express Tribune." The Express Tribune, 2 Apr. 2022, tribune.com.pk/story/2350667/gang-involved-in-child-pornography-busted.

39 The Internet Watch Foundation (IWF) is a UK-based charity that works to identify and remove child sexual abuse content from the internet. It also provides a hotline for the public to report such content and works with law enforcement agencies to combat the distribution of such material.

40 "New Data Published by IWF Shows Girls Are at Increasing Risk Online." New Data Published by IWF Shows Girls Are at Increasing Risk Online, www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-girls-online-at-record-high-following-pandemic-lockdowns. Accessed 17 Nov. 2022.

boys and girls can be victims of online violence and abuse, girls are significantly more likely to be victims of repeated and severe forms of technology-facilitated violence against children that affect their safety, physical and mental health, livelihoods, family ties, dignity, and reputation. The Internet Watch Foundation has also revealed that the number of "self-generated' sexual imagery of 7 to 10-year-olds increased by 360% between 2020 and 2022[41].

A study conducted by the Digital Rights Foundation in Pakistan found that girls' online experiences differ significantly from those of boys[42]. Several female respondents reported being followed and approached by older men. Girls reported being more likely to be harassed by men online, for example through repeated inbox messages or by being sent lewd photos.

The statistics on OCSEA available from the FIA are limited and could be improved. This is very important because awareness of the extent of OCSEA remains low among key stakeholders in Pakistan. This leads to a low sense of urgency and is likely to result in the issue of OCSEA receiving limited political attention and funding. In order to develop effective and appropriate responses, it is important that the federal and provincial governments have a clear understanding of the extent, characteristics and trends of OCSEA in all provinces and regions. This requires that all relevant government agencies regularly collect and publish statistics on prevalence disaggregated by gender and age, and share this information with key stakeholders as evidence to improve policies and strategies to tackle OCSEA.

41 V. (2024, January 29). *Global Threat Assessment 2023 - WeProtect Global Alliance*. VerifyMy News. https://verifymy.io/blog/global-threat-assessment-2023/

42 YOUNG PEOPLE and PRIVACY IN ONLINE SPACES. Digital Rights Foundation (DRF), 2021.

Threats and Dangers for Children in the Digital World

The risks to which children are exposed when using ICT are many and varied. Children who use ICT excessively and are not supervised are at high risk of being exposed to sexual content that is easily accessible online. Exposure to such explicit content increases children and young people's vulnerability to sexual abuse and exploitation. This can also lead to children developing various 'sexual illiteracies' and viewing such behaviour as normal and acceptable due to the lack of communication and discussion on the topic[43]. This makes children an easy target for predators who lure children to produce child sexual abuse material. Since many children are not aware of the biological aspects of their bodies, the sexual arousal of viewing pornography can trigger feelings of guilt and anxiety in the child[44]. Unfortunately, pornography, sexual abuse of children and cyber crimes against children are issues that are rarely discussed in Pakistan due to the shame and stigma associated with them. If a child is exposed to sexual content at a very young age, he or she may become de-sensitied to sex and be tempted to engage in sexual behaviour at a young age.

Moreover, ICT provide a platform where children can easily meet strangers. According to one survey, more than 40 per cent of children chat online with strangers on social media and gaming platforms that they would never meet in real life (Cybersafe Kids 2019). Children are particularly vulnerable to being manipulated by adults they meet online. Once an online relationship is established, the groomer often steers the conversation towards sex. The child may be pressured into taking explicit photos or videos of themselves and sending them to the groomer. Many think this is fun and safe at first, partly because they trust the person and do not meet the person in person. After the criminals have one or more videos or images, they threaten to publish this content online, or they threaten violence to get the victim to produce more images. The shame, fear and confusion children feel when caught in this cycle often prevents them from asking for help or reporting the abuse[45].

43 Lin, Wen-Hsu, et al. "Exposure to Sexually Explicit Media in Early Adolescence Is Related to Risky Sexual Behavior in Emerging Adulthood." PubMed Central (PMC), 10 Apr. 2020, www.ncbi.nlm.nih.gov/pmc/articles/PMC7147756.

44 "The Impact of Seeing Online Pornography on Children | Digital Parenting App | Canopy Aus." Digital Parenting App | Canopy Aus, 30 Nov. 2021, mycanopyapp.com/2021/11/the-impact-of-seeing-online-pornography-on-children.

45 FBI Issues Alert on Increased Child Sextortion Nationwide - Prensa Latina." Prensa Latina - Latin American News Agency, 20 Dec. 2022, www.plenglish.com/news/2022/12/20/fbi-issues-alert-on-increased-child-sextortion-nationwide.

Stages of Online Grooming

Grooming, unlike most other forms of child sexual abuse (CSA), is often an insidious process. Although grooming is case-specific and looks different for each victim, the following stages can be observed in most cases[46].

1. Targeting: Perpetrators seek out children by creating false profiles on the internet, often by pretending to be a child in the same age group and contacting them online. Often the perpetrators target children in their close circle of friends or family.

2. Gaining access: The perpetrator builds trust with the child by making them feel special, sometimes through gifts or excessive compliments and attention.

3. Trust Development: The perpetrator becomes a constant presence in the child's life and gives the appearance of a friendly or even romantic relationship.

4. Desensitisation to sexual content and touch: Once a certain level of trust has been established, the groomer begins to desensitise the child to touch and sexual content, for example by establishing physical proximity or exposing the child to sexual content, in order to create an environment for child sexual abuse (CSA) and child sexual exploitation.

5. Maintaining control: Perpetrators often use secrecy and feelings of shame to maintain control over the child. In some cases, perpetrators use self-created intimate content to blackmail children into prolonging the abusive relationship.

Source: INHOPE[47]

46 "The Stages of Grooming." INHOPE, www.inhope.org/EN/articles/the-stages-of-grooming. Accessed 8 Jan. 2023.

47 *INHOPE* | https://www.inhope.org/

It is important to recognise that OCSEA is also related to offline sexual exploitation and abuse of children, as some individuals may use the internet or other technologies to facilitate their offline abuse, for example by grooming children through online platforms or using the internet to find and contact children to exploit them.

Co-occurrence of Online and Offline Child Sexual Abuse

A 15-year-old boy, Grade 8 student, narrated in a witness statement[48] that he was introduced to the offender by his friend, who later started taking pictures on his mobile phone and over time he lured the victim and took nude pictures of him, after which the offender started blackmailing him to satisfy his unnatural lust. The victim also narrated details of how he was taken to different places where the abuser blackmailed him, committed unnatural offences and made nude films.

While some child sexual abuse material depicts children in great distress and the sexual abuse is obvious, other images or videos show children who appear complacent[49]. However, just because a child appears unconcerned does not mean that sexual abuse has not taken place. Often, perpetrators "groom" their victims, i.e. they build a relationship with a child and gradually sexualise contact with them[50]. Most often, the abuse is an ongoing victimisation that goes on for months or years, rather than a single incident. In order to desensitise a child or weaken their resistance to sexual abuse, a false sense of trust and authority is built up towards the child. Therefore, it is important to keep in mind that the abuse may have started earlier than the image was created, even if the child seems comfortable in it.

The production of child sexual abuse material (videos, images, etc.) creates a permanent record of a child's sexual abuse. Victims of online child sexual exploitation and abuse suffer not only from the sexual abuse inflicted on them to produce child sexual abuse content, but also from the knowledge that their images and videos can be traded and viewed by others worldwide. Once the

48 Sighted by MSK v. The State [2022] Islamabad High Court, Criminal Appeal No. 151/2020

49 Ibid.

50 "Examples of Grooming in Child Sexual Abuse." Grewal Law PLLC, 20 Sept. 2021, www.4grewallaw.com/blog/2021/september/examples-of-grooming-in-child-sexual-abuse.

material is published on the internet, it is irretrievable and can continue to circulate without any control[51].

Victims are often re-victimised for the rest of their lives, knowing that the images and videos will be available on the internet forever[52]. The children who are exploited in these images have to live with the permanence, longevity and spread of such a record of their sexual abuse. This often leads to long-term psychological damage to the children, including disruption of sexual development, self-image and the development of trusting relationships with others in the future. Many victims of OCSEA suffer feelings of helplessness, fear, humiliation, and lack of control as their images are forever visible to others[53].

OCSEA affects children of all ages, backgrounds, socio-economic status, gender and vulnerability. The perpetrators can come from all countries, regardless of age and gender. It is important that parents, educators, and caregivers educate children about these risks and help them use technology safely and responsibly. This includes setting appropriate limits on screen time, monitoring online activity, using parental control tools to filter content and restrict access to certain websites and apps, and ensure dialogue with children about such issues, and a parental awareness on how to react and what to do – and not to do- if the child discloses any threat or abuse experienced online.

51 "Child Pornography." Child Pornography, 26 May 2015, www.justice.gov/criminal-ceos/child-pornography.

52 Ibid.

53 Ibid.

International Legal Framework for Child Online Protection

International human rights law can provide guidance to State parties on international standards and, accordingly, help them enact adequate laws, notify relevant policies and design necessary programmes to curb violence against children committed through the use of ICT, in line with relevant international best practices.

Convention on the Rights of the Child (CRC), 1989

The CRC[54], is the most widely ratified international human rights treaty, sets out the civil, political, economic, social and cultural rights of children. Pakistan ratified the Convention in 1990.

The Convention protects children from all forms of violence, exploitation, and abuse, and from discrimination of any kind, and ensures that the best interests of the child should be a primary consideration in all matters affecting him or her. Article 34 of the CRC requires States Parties to take all appropriate measures to protect children from all forms of sexual exploitation and abuse, including measures to prevent the exploitative use of children in pornographic performances and materials.

General Comment No. 25 (2021) on Children's Rights in relation to the Digital Environment

The CRC does not explicitly mention the online protection of children from abuse and exploitation[55]. Therefore, on 24 March 2021, the United Nations Committee on the Rights of the Child adopted General Comment No. 25 on children's rights in relation to the digital environment. This General Comment supports the assertion that children's rights apply online as well as offline.

The General Comment No. 25 provides guidance on how States Parties should interpret and implement the Convention on the Rights of the Child through legislative, policy and other measures to ensure that States fully comply with their obligations under the Convention on the Rights of the Child[56]. In the context of the digital environment, the GC No. 25 places particular emphasis on the rights to freedom of expression, privacy, and non-discrimination. It also identifies the need

54 *Convention on the Rights of the Child*. www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

55 Malik, Advocate Wajahat Ali. "Protection of Digital Rights of Children." *Pak Observer*, pakobserver.net/digital-rights-of-children-by-wajahat-ali-malik

56 ibid

for children to have access to digital literacy education and safe online spaces, and the importance of protecting children from OCSEA.

GC No. 25 on children's rights in relation to the digital environment was drafted after a participatory process to take into account the views of children, and Pakistani children were among the group of children who gave their input to the CRC Committee through online consultations jointly organised by CSOs and the NCRC, as well as through participatory research with children involving Pakistani children, CSOs and the NCRC in collaboration with the University of Sydney

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC), 2000

The OPSC is one of the most important international legally binding instruments containing provisions obliging States Parties to criminalise illegal acts related to child sexual abuse material[57].

Child sexual abuse material (CSAM) is referred to as "child pornography" in Article 2 of the OPSC and is defined as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes (Art. 2 (c))"

Article 3 (1) (a) of the OPSC states that each State Party shall ensure that, as a minimum, the acts of producing, distributing, disseminating, importing, exporting, offering, selling, or possessing for the above purposes child pornography (now referred to as CSAM) as defined in Article 2 of the OPSC shall be fully covered under "its criminal or penal law", whether such offences are committed domestically or transnationally or on an individual or organized basis.

Article 3 (1) (c) of the OPSC requires State Parties to criminalise acts related to child pornography whether committed domestically or transnationally, on an individual or organised basis including producing, distributing, disseminating,

57 *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*. www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child. Accessed 11 Nov. 2022.

importing, exporting, offering, selling child pornography (now referred to as CSAM) or possessing it for the purpose of production, distribution, dissemination, importation, exportation, offer, or sale.

Article 3 (3) of the OPSC obliges State Parties to make such offences punishable by appropriate penalties that take into account their grave nature.

Article 3 (4) of the OPSC mandates State Parties to take measures, whether appropriate, to establish liability of legal persons for offences established in its Article 3 (1), subject to the provisions of their national laws and such liability may be criminal, civil, or administrative.

Article 4 (2) of the OPSC stipulates that a State Party may take such measures as may be necessary to establish extraterritorial jurisdiction over the offences referred to in

Article 3 (1) in one of the following cases: (a) when the alleged offender is a national of that State or a person who has habitual residence in its territory; or (b) when the victim is a national of that State.

Article 7 (a) of the OPSC states that State Parties shall, subject to the provisions of their national law, take measures to provide for: (i) the confiscation of assets used to commit or facilitate offences under the present protocol; and (ii) the confiscation of proceeds derived from such offences.

Pakistan ratified the OPSC in 2011 and is thus obliged to implement these instruments and report on progress to the UN Committee on the Rights of the Child in Geneva every five years. The first report, due in 2013, was submitted by Pakistan in September 2019. As of December 2022, the Committee has not yet released its concluding observations.

The Government of Pakistan report submitted under article 12 (1) of OPSC highlights various steps taken by the Government of Pakistan, such as amending the Pakistan Penal Code, 1860 ("PPC") and the Code of Criminal Procedure, 1898, through the Criminal Law (Amendment) Act, 2016, to protect the child by criminalizing acts such as child trafficking, child prostitution, child pornography and the sale of children. Child pornography (now referred to as CSAM) has been criminalised in Section 292-C of the PPC[58]. The report shows that the Government of Pakistan provides mutual legal assistance in criminal matters on the basis of bilateral treaties and international conventions to which Pakistan and the State requesting assistance are parties. The mechanism is enshrined in the Code of Criminal Procedure 1898. The report mentions that a National Human Rights Action Plan has been in place since 2016, which includes measures related to children's rights. Under the Action Plan, a National Policy Framework on Human Rights is being developed by the Ministry of Human Rights to protect human rights, including the protection of children from abuse, violence, discrimination and exploitation, including the sale of children, child prostitution and child pornography.

Committee on the Rights of the Child issued Guidelines regarding the Implementation of the OPSC

The Committee on the Rights of the Child has long been concerned that many States Parties are not properly implementing the OPSC and that the Protocol needs to be adapted to cover online exploitation[59]. In response, the Committee released a new set of guidelines in 2019 to provide concrete advice to States on how to effectively protect children from OCSEA. These guidelines[60] take into account various current trends and issues, such as:

58 Section 292C of PPC, which prescribed penalties for child pornography, were repealed by the Criminal Law Amendment Act 2023 and addressed in PECA 2016

59 "UN Urge States to Treat Sexually Exploited Children as Victims, Not Criminals." *ECPAT*, 19 Oct. 2021, ecpat.org/opsc-guidelines-un-ecpat.

60 *CRC/C/156: Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.* (n.d.). OHCHR. https://www.ohchr.org/en/documents/legal-standards-and-guidelines/crcc156-guidelines-regarding-implementation-optional

- The OPSC guidelines offer suggestions to State parties on how to deal with the increasing number of sexually explicit images/videos produced by children themselves. It is emphasised that children should never be held responsible for the disclosure of these materials.

- The new guidelines emphasise the need for stronger and more effective education programmes to help children access support groups and should include the use of tech-friendly platforms to educate children, parents, school teachers and caregivers about online abuse.

- The guidelines provide recommendations on how states can improve their legal systems to ensure that sexually exploited children are treated as victims and not as criminals.

- These guidelines also highlight the pivotal role that businesses play in combating the sexual abuse and exploitation of children. Banks must work to stop payments, internet service providers should block illegal sites and increase their cooperation with law enforcement, the travel and tourism industry should work to prevent their services from being abused by criminals, to name a few

- Other issues raised in the guidelines include gender-sensitive victim support programmes, especially for boys, and more attention should be paid to protecting vulnerable groups of children.

An Inter-agency Working Group[61] has produced an Explanatory Report[62] which supplements the Guidelines and provides more detailed information and specific examples of the implementation of certain provisions of the OPSC. The Explanatory Report follows the structure and includes the integral text of the OPSC Guidelines. For each paragraph of the Guidelines, additional information is added regarding the different issues raised, and references are included to international and regional standards linked to the issues covered under the OPSC, the Committee's relevant General Comments, and recommendations by

61 The inter-agency working group consists of ECPAT International, the Office of the High Commissioner for Human Rights, ITU, the Secretariat of the CRC Committee, UNICEF, UN Special Rapporteur on the Sale and Sexual Exploitation of Children, UN Special Representative of the Secretary General on Violence against Children, Children's Rights Division - Secretariat of the Lanzarote Committee, Council of Europe, International Centre for Missing and Exploited Children (ICMEC), among others.

62 Interagency Working Group. (2019, September). *Explanatory Report to the Guidelines regarding the implementation of the OPSC*. https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/OPSC-Guidelines-Explanatory-Report-ECPAT-International-2019.pdf

other similar bodies. The report is detailed and useful for States in establishing sound child protection systems.

Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure

The Optional Protocol on a Communications Procedure (OPCP)[63] recognises that children have the right to appeal to an international mechanism specific to them when national mechanisms are unable to address violations effectively. Pakistan has not ratified this Optional Protocol by Jan 2023.

ILO Convention on the Worst Forms of Child Labour, 1999 (No. 182)

In 1999, the International Labour Organization (ILO) adopted the Convention on the prohibition and immediate action to eliminate the worst forms of child labour[64]. Pakistan ratified this Convention on 11 October, 2001. Articles 1 and 3 (b) of the Worst Forms of Child Labour Convention, 1999 (No. 182) require States Parties to take immediate and effective steps to ensure the prohibition and elimination of the use, procuring, or offering of a child for the production or performance of pornography.

Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children supplementing the United Nations Convention against Transnational Organized Crime

In November 2022, Pakistan has ratified the Protocol to Prevent, Suppress and Punish Trafficking in persons Especially Women and Children, supplementing the UN convention against Transnational Organized Crime[65] (UN Trafficking Protocol) with two reservations[66]. The Protocol establishes the first common international

63 *Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure.* www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-communications.

64 "C182 - Worst Forms of Child Labour Convention, 1999." *https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182.* Accessed 27 Nov. 2022.

65 *Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime.* www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons. Accessed 22 Nov. 2022.

66 "UNTC." *UNTC*, treaties.un.org/Pages/ViewDetails.aspx?src=ind&mtdsg_no=XVIII-12-a&chapter=18&clang=_en. Accessed 19 Nov. 2022.

definition of trafficking in persons". It aims to prevent and combat this crime and facilitate international cooperation against it. The Protocol also highlights the problems associated with trafficking in persons, which often leads to inhumane, degrading and dangerous exploitation of trafficked persons

ECOSOC Resolution 2011/33

The UN Economic and Social Council issued a resolution[67] entitled "Economic and Social Council Resolution 2011/33 on prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children". The resolution emphasises that new information and communication technologies and applications are being misused to commit crimes of child sexual abuse and exploitation. Furthermore, the ECOSOC resolution highlights that technological developments have enabled the emergence of crimes such as the production, distribution, or possession of child sexual abuse images, audio or video, exposure of children to harmful content, grooming, harassment, and sexual abuse of children, and cyber-bullying.

Budapest Convention

The Convention on Cybercrime ("Budapest Convention")[68] is considered to be a comprehensive and coherent intergovernmental instrument on cybercrime and electronic evidence dealing with computer-assisted offences in the area of child pornography. The treaty is open for accession by any country. Pakistan has not adopted the Budapest Convention.

It serves as a guide for all countries developing domestic legislation on cybercrime and as a framework for international cooperation among States Parties to this Convention. Article 9 of the Cybercrime Convention contains provisions that criminalize child pornography offences committed through the use of a computer system, provided that such commission is intentional and unauthorized. The Budapest Convention provides for the criminalization of conduct - ranging from illegal access, data and system interference to computer-related fraud and child pornography, as well as procedural powers to investigate cybercrime and secure electronic evidence related to any crime and for efficient international cooperation.

67 "Prevention, Protection and International Cooperation Against the Use of New Information Technologies to Abuse and/or Exploit Children." *https://www.un.org/en/ecosoc/docs/2011/res%20 2011.33.pdf.* Accessed 21 Nov. 2022.

68 "Budapest Convention." *Cybercrime*, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 15 Nov. 2022.

The Convention is supplemented by a First Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS 189) and a Second Additional Protocol on enhanced international cooperation and disclosure of electronic evidence (CETS 224) which was opened for signature on 12 May 2022[69].

Lanzarote Convention

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (also known as the Lanzarote Convention)[70] contains provisions on offences related to child pornography (Article 20) and online grooming (Article 23). Lanzarote Convention is open for ratification by Council of Europe member states. Additionally, this Convention is open for accession by non-member States of the Council of Europe.

Rio de Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and Adolescents

The World Congress III against the Sexual Exploitation of Children and Adolescents was held in Rio de Janeiro, Brazil, from 25to 28 November 2008 to review the development and actions taken following the Stockholm Declaration and Agenda for Action (1996) and the Yokohama Global Commitment (2001). A document entitled "Rio de Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and Adolescents" ("Rio de Janeiro Pact")[71] was produced. Although this document is not an international legally binding instrument, it addresses measures to be taken at national level to prevent, prohibit and criminalize certain forms of sexual exploitation of children and adolescents. A particular focus is on the abuse of children and young people through the Internet and related technologies, including activities related to child sexual abuse material and grooming of children committed through the use of the Internet and new technologies.

69 Ibid.

70 "Lanzarote Convention." *Children's Rights*, www.coe.int/en/web/children/lanzarote-convention. Accessed 28 Nov. 2022.

71 *The Rio De Janeiro Pact to Prevent and Stop Sexual Exploitation of Children and Adolescents*. polis.osce.org/rio-de-janeiro-pact-prevent-and-stop-sexual-exploitation-children-and-adolescents. Accessed 27 Nov. 2022.

Sustainable Development Goals (SDGs)

The 2030 Agenda for Sustainable Development (the 2030 Agenda) is a set of international development goals for the period from 2016 to 2030, adopted at the UN Sustainable Development Summit in September 2015, building on the success of the Millennium Development Goals (MDGs). The Sustainable Development Goals 2016-2030[72] provide a framework for action by governments in their efforts to protect children from offline and online abuse and exploitation. This global commitment, to which the Government of Pakistan has agreed, provides for the protection of children from all forms of violence under Goal 16.2 and other related goals, i.e. 5.2 and 8.7. This includes abuse, exploitation, trafficking, harmful practices and neglect or negligent treatment.

There are a number of challenges in applying the international human rights framework domestically, particularly in the protection of privacy and the regulation of content, which can lead to inconsistencies in approaches to protecting children online from OCSEA. Regulations for digital service and platform providers are inconsistent and each country applies its own national laws when assessing reported content, which can be easily exploited by perpetrators, and a fragmented regulatory landscape can exacerbate these risks by making it easier for perpetrators to evade detection and prosecution. Additionally, the complexity of cybercrimes, evolving technology and the challenges of international co-operation further complicate the development of enforceable international laws to combat OCSEA.

72 *THE 17 GOALS | Sustainable Development*. sdgs.un.org/goals. Accessed 30 Nov. 2022.

Pakistan's Legal Framework for Child Online Protection

This section provides an overview of Pakistan's national and provincial laws dealing with COP.

Constitution of Pakistan, 1973

The Constitution of the Islamic Republic of Pakistan, the supreme law of Pakistan, undertakes in "Article 3" to ensure the elimination of all forms of exploitation and the protection of law as the inalienable right of every citizen. "Article 11" of the Constitution prohibits all forms of slavery, forced labour, human trafficking, employment of children under 14 years of age and work of children in hazardous conditions. "Article 25" states that all citizens are entitled to equal protection under the law and empowers states to make special provisions for the protection of women and children. "Article 35" provides that the state shall protect the family and children. "Article 37(e)" provides that the state shall make provision for securing just and humane conditions of work, ensuring that children and women are not employed in vocations unsuited to their age or sex, and for maternity benefits for women in employment.

Pakistan Penal Code, 1860

The Pakistan Penal Code, 1860 (PPC) is the main criminal code of Pakistan. There are several provisions in the PPC that are relevant to OCSEA. "Sections 292A, 293 and 294" of the PPC deal with the sale, distribution and public exhibition of obscene books circulated in any manner, exposure to seduction of children, sale of obscene objects to young person, and obscene acts and songs. *"Section 292B" and "Section 292c", which previously defined child pornography and prescribed penalties for child pornography, were repealed by the Criminal Law Amendment Act 2023 and addressed in the PECA 2016.*

"Section 292A" of the PPC deals with exposure to seduction. Whoever, by any means, seduces a child with intent to involve him in any sexual act or exposes him to any obscene and sexually explicit material, document, film, video or computer generated image or attempts to commit the aforesaid act, shall be punished with imprisonment for a term which shall not be less than one year and which may extend to seven years or with fine which shall not be less than one hundred thousand rupees and which may extend to five hundred thousand rupees or with both.

"Section 293" of PPC prohibits the sale, distribution, exhibition, or circulation of obscene objects to young person under the age of twenty and is punishable by imprisonment for a term not exceeding six months or by a fine, or by both.

Cruelty to a child is dealt with under "Section 328A" of the PPC. Cruelty is defined as willful assault on a child, ill-treatment, neglect or abandonment of a child or any act which results or is likely to result in physical or psychological injury to a child. Whoever commits the offence intentionally shall be punished with imprisonment for a term which shall not be less than one year and not more than three years or with fine which shall not be less than twenty-five thousand rupees and not more than fifty thousand rupees or with both.

"Section 377A" of the PPC deals with sexual abuse of children which states that whoever employs, uses, coerces, persuades, induces, entices or compels any person to grope, fondle, caress, engage in exhibitionistic acts, voyeurism or other obscene or sexually explicit acts or the simulation of such acts either independently or in conjunction with other acts, with or without consent, if the person is less than eighteen years of age, commits the offence of sexual abuse. Sexual abuse has been criminalised in "Section 377B" of the PPC 1860, which states that the person who commits the offence of sexual abuse shall be punishable with imprisonment for a term which shall not be less than fourteen years and may extend up to twenty years and with fine which shall not be less than one million rupees.

Prostitution is illegal in Pakistan and has been criminalised. "Section 371A" and "Section 371B" of the PPC criminalise the sale or purchase of a person for the purpose of prostitution, punishable by imprisonment for up to 25 years and a fine. "Section 366A" of the PPC criminalises the procuration of minor girls under the age of 18 for illicit sexual intercourse, punishable by imprisonment of up to 10 years and a fine.

The Prevention of Electronic Crimes Act (PECA), 2016

PECA 2016 contains specific procedural measures that apply to all cybercrime investigations, crimes committed using computer systems and all criminal investigations where digital evidence is required. The PECA 2016 also applies to cases related to the OCSEA. The law is enforced throughout Pakistan.

The Criminal Laws (Amendment) Act, 2023, passed in July 2023, made important changes to the PECA 2016 and enhanced the scope of the law, including tougher penalties, improved protection for children, streamlining investigation procedures by allowing police to take cognizance of offences under the PECA, the composition of a joint investigation team and providing protection to victim and witness. It also amended the Qanoon-e-Shahadat[73] regarding the admissibility of witness statements taken by the court through modern devices or techniques, including video calls, viber, skype, WhatsApp, facebook, etc.

The amendments to the PECA 2016 contain important additions to the definitions. of harmful content, non-sexual child abuse and sexually explicit conduct. Firstly, the age of a "child" has been defined as a person under the age of eighteen. Secondly, the term "child sexual abuse content" is now defined to include depictions of a child engaged in real or simulated sexually explicit conduct or the depiction of a child's body parts for primarily sexual purposes. Additionally, the definition of "sexually explicit conduct" has been broadened to include a range of real or simulated activities, including various forms of sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse and lascivious exhibition of certain body parts.

PECA 2016: OCSEA Offences and Penalties

- "Section 20" of the PECA 2016 deals with offences against the dignity of a person in the context of information shared through information systems. If someone intentionally spreads false information about a person through any digital platform, knowing it can harm that person's reputation or privacy, they can face punishment. The punishment could be imprisonment for up to three years, a fine of up to one million rupees, or both.

73 Qanoon-e-Shahadat, also known as the law of evidence, is a legal framework that governs the rules and procedures relating to the presentation and admissibility of evidence in the legal system of Pakistan. The law of evidence is mainly codified in the Qanoon-e-Shahadat Order, 1984.

- "Section 21" of the PECA 2016 relates to modesty of a minor and a natural person. It prescribes imprisonment up to seven years and fine up to five million rupees in case a person is involved in online child abuse.
- "Section 22" of the PECA 2016 deals with child pornography and makes it a serious offence to intentionally produce, offer, distribute, or possess material that depicts minors engaged in sexually explicit conduct. Those found guilty may face imprisonment from fourteen to twenty years and a fine not less than one million rupees.
- "Section 22A" of the PECA 2016 deals with online grooming, solicitation, and cyber enticement. This section addresses intentionally creating a relationship of trust with a minor through digital means with the intent to commit sexual abuse or share explicit content. The punishment includes imprisonment ranging from five to ten years and a fine from five hundred thousand to ten million rupees.
- "Section 22B" of the PECA 2016 deals with commercial sexual exploitation of children which pertains to involvement in using digital means for the sexual exploitation of minors. The penalty is imprisonment for a minimum of fourteen years up to twenty years and a fine not less than one million rupees.
- "Section 22C" of the PECA 2016 deals with the use of information system for kidnapping, abduction, or trafficking of minor. According to this section, anyone who contacts a minor with the intent to kidnap, abduct, or traffic for sexual abuse or exploitation faces imprisonment for a minimum of fourteen years up to twenty years and a fine not less than one million rupees.
- "Section 24" of the PECA 2016 deals with cyberstalking which means anyone using digital platforms to harass, intimidate, or coerce someone. The penalty includes imprisonment for up to three years, a fine up to one million rupees, or both. For offences against minors, the punishment may extend to five years, a fine up to ten million rupees, or both.

- "Section 24A" of the PECA 2016 deals with cyberbullying which means anyone harassing or threatening someone through electronic messages on social media platforms. The penalty includes imprisonment for up to five years, not less than one year, a fine of up to five hundred thousand rupees, and not less than one hundred thousand rupees.

- "Section 25" of the PECA 2016 deals with issue of spamming which means anyone transmitting harmful or unsolicited information without permission. Offenders may face imprisonment for up to three months, a fine of up to five million rupees, or both. For direct marketing violations, fines range from not exceeding fifty thousand rupees for the first offence to not less than fifty thousand rupees and up to one million rupees for subsequent violations.

- "Section 30" of the PECA 2016 outlines the authority and process for investigating offences under the Act. Besides the FIA, the Police are now also authorised to handle these offences. However, the Police must promptly refer the matter to the FIA for technical opinions and investigations as per its rules. Additionally, the Federal or Provincial Government can form joint investigation teams. The investigation must be completed within forty-five working days for cases triable by the court. Once the court takes cognizance of a case, it must proceed with a weekly trial and make a decision within three months.

- "Section 30B" of the PECA 2016 provides protection to victims and witnesses involved in cases to ensure the safety and well-being of individuals participating in legal proceedings related to offences covered by the Act.

- "Section 30C" of the PECA 2016 specifies that trials for offences against minors be conducted privately (in-camera), ensuring the proceedings are not open to the public and the court may adopt protective measures to shield victims and witnesses. Publishing or broadcasting proceedings are not allowed without the court's permission.

- "Section 30D" of the PECA 2016 is related to the investigation referred to the PTA related to child sexual abuse content. This section outlines that the FIA is responsible for obtaining information about child sexual abuse content referred for blocking and removal by the PTA and other relevant organizations.
- "Section 34" of the PECA 2016 provides for general measures of international cooperation, including comprehensive provisions on spontaneous information, grounds for refusal, confidentiality and limitations on use, as well as authorisations to cooperate on specific investigative measures.
- "Section 43" of the PECA 2016 specifies that offences under "Sections 10, 21, 22, 22A, 22B, and 22C", along with abetment of these offences, are non-bailable, non-compoundable, and cognizable by the investigation agency. *Non-bailable means that individuals charged with these offences are not eligible for bail by default. Non-compoundable implies that the complainant cannot withdraw the charges. Cognizable means that the investigation agency can make arrests without a warrant.*
- "Section 43A" of the PECA 2016 deals with complaint against cybercrimes against children where individuals can file complaints against specific cybercrimes targeting children under "Sections 10, 21, 21A, 21B, 21C, 21D, 21E, and 21F", as well as abetment of these offences to the relevant authorities. This section establishes a specific procedure for reporting and seeking resolution for cybercrimes that victimise children.
- "Section 45A" of the PECA 2016 section mandates the government to develop a support mechanism for victims in collaboration with other agencies and civil society organizations.

The PECA, 2016 also includes number of other sections that may be associated with OCSEA cases, including unauthorised access to information systems or data ("Section 3"), unauthorised copying or transmission of data ("Section 4"), electronic fraud ("Section 14"), making, supplying or obtaining devices for use in offences ("Section 15"), defamation ("Section 20"), special protection of women ("Section 21"), spamming ("Section 25") and spoofing ("Section 26"), offences committed in relation to information systems ("Section 27"), expedite preservation and acquisition of data ("Section 31"), Retention of traffic data ("Section 32"), Powers of an authorised officer ("Section 35"), Dealing with seized data or information system ("Section 36"), unlawful on-line content ("Section 37"), real-time collection and recording of information ("Section 39").

Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules, 2021

The Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021 ("Rules") have been approved to implement "Section 37" and "Section 51" of the PECA, 2016. "Sections 37 and 51" of the PECA provide that the Pakistan Telecommunication Authority (PTA) may make rules for blocking and regulating online content on social media forums. The section also provides that such content shall be blocked and removed if PTA is of the opinion that it is against the honour and interests of Islam, the defence, security and integrity of Pakistan, public order, decency or morality, or is in connection with contempt of court or the commission or incitement of an offence relating to data protection or cybercrime.

Social media or social networking services are defined in the Rules as a website, application or mobile web application, platform or communication channel and any other such application and service that permits a person to become a registered user, create an account or create a public profile for the primary purpose of, allowing the user to post and share user-generated content through such account or profile, or to enable one or more users to generate content that can be viewed, posted and shared by other users of such platform, but does not include the licensees of PTA unless they specifically provide social media or social networking services. A social media company could face a penalty of

up to 500 million rupees if it fails to comply with the direction of the Pakistan Telecommunication Authority (PTA) for blocking online content[74].

"Section 3" of the Rules is important because it describes the cases where removal of online content is permitted under "Section 37" of the PECA 2016, which may lead to the blocking and removal of online content that offends decency and morality where the online content constitutes an act that is an offence under "Sections 292, 293, 294 and 509" of the Pakistan Penal Code. ("Section 292" and Section "294" deal with selling obscene books and articles, as well as performing obscene songs and acts in public. "Section 509" deals with insulting a woman's modesty or sexual harassment.) Service providers, social media companies, and major social media companies are required to place mechanisms for immediate blocking of live streaming of online content through Pakistan's online information system, particularly if they receive a notice from PTA of content relating to terrorism, hate speech, pornography, incitement to violence, and endangering national security.

Service Providers Liability

A very important issue is the obligation and liability of service providers. Pakistan's PECA 2016 does not impose any obligation on service providers, including ISPs, to monitor, block and remove CSAM and is not required to report CSAM to the relevant authorities. However, under "Rule 7(5)" of the Removal Blocking of Unlawful Online Content Rules 2021, service provider shall deploy mechanisms to ensure the immediate blocking of online streaming, including pornographic content, and under "Section Rule 7(4)", service provider shall provide information with the designated investigative agency. However, this rule appears to contravene "Section 38(5)" of PECA 2016, which deals with the limitation of liability of service providers. It states that no service provider shall be under any obligation to proactively monitor make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by any such intermediary or service provider.

74 Govt Issues Rules for Removal, Blocking of Unlawful Online Content. 28 Dec. 2022, www.thenews.com.pk/print/900332-govt-issues-rules-for-removal-blocking-of-unlawful-online-content.

Given the significant intersection between the online and offline worlds, it's important to recognise that various laws may apply to protect victims and hold perpetrators accountable in some cases of OCSEA, including:

The Anti-rape (Investigation and Trial) Act, 2021

The Anti-rape (Investigation and Trial) Act, 2021 was enacted to ensure expeditious redressal of rape and sexual abuse crimes concerning women and children. It establishes special investigation teams and special courts to facilitate efficient procedures, speedy trials, evidence collection, and related matters, emphasizing the need for swift justice in such cases.

Prevention of Trafficking in Persons Act, 2018

Prevention of Trafficking in Persons Act, (PTPA) 2018 aims to prevent trafficking in persons especially women and children. "Section 3(1)" of the PTPA 2018 specifies that any individual who engages in activities such as recruiting, harbouring, transporting, providing, or obtaining another person for compelled labour or commercial sex acts through the use of force, fraud, or coercion commits this offence. The prescribed punishment for such offences includes imprisonment for a period of up to seven years, a fine of up to one million rupees, or both. Moreover, if the offence of trafficking in persons is perpetrated against a child or a woman, the severity of the penalties increases. In such cases, the perpetrator is subject to imprisonment for a term not exceeding ten years, with a minimum sentence of two years, a fine of up to one million rupees, or both.

Islamabad Capital Territory and Provincial Laws

Islamabad Capital Territory Child Protection Act, 2018

The ICT Child Protection Act, 2018 provides for the protection and care of children in the Islamabad Capital Territory from all forms of physical or mental violence, neglect, maltreatment, exploitation and abuse through the establishment of Child Protection Advisory Board and Child Protection Institutes.Advisory Board.Key functions of the Child Protection Advisory Board include advising the government on policy and legislation, ensuring coordination of implementation of child protection and care mechanisms, and maintaining a management information system for child protection. Child Protection Institutions under the Act has the mandate to receive reports of children in need, maintain case management records, and collect data on child abusers and offenders against children. The Act

defines sexual abuse and exploitation as causing or coercing a child to engage in unlawful sexual activity, including the use of children in audio or visual images for child pornography, child protection, trafficking within and between countries for sexual exploitation and sale of children for sexual purposes.

Khyber Pakhtunkhwa Child Protection and Welfare Act, 2010

The Khyber Pakhtunkhwa Child Protection and Welfare Act, 2010 provides for the care, protection, maintenance, welfare, training, education, rehabilitation, and reintegration of children at risk in Khyber Pakhtunkhwa. for Section 2e(Vi) defines child pornography, including online child pornography as "taking, permits to be taken, with or without the consent of the child, any photograph, film, video, picture or representation, portrait, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of obscene or sexually explicit conduct."

"Section 35" deals with frauding or deceiting a child by words, spoken or written, or by signs or otherwise, incites, attempts to incite, deceits or allows a child to engage in any activity which is harmful to the physical, mental, emotional, economic and social well-being of a child, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one hundred thousand rupees or with both. "Sections 36" and "Sections 37" deal with violence against a child that causes or intends to cause harm, pain, suffering or humiliation to a child. "Section 40" of the Act defines the offences, while "Section 48" sets out the punishment for child pornography, which is up to seven years imprisonment with a minimum sentence of three years and a fine. "Section 50" deals with the offence of exposing a child to seduction with intent to engage him in a sexual act or exposing him or attempting to expose him to obscene and sexually explicit material, document, film, video or computer-generated performance and is punishable with imprisonment for a term which may extend to seven years or with fine which may extend to ten thousand rupees or with both. Sexual abuse of children is dealt with in "Section 53" and can be punished with up to 14 years.

KP Child Protection and Welfare Act, 2010
"Section (f)" - Child Pornography

"child pornography" means taking, permits to be taken, with or without the consent of the child, any photograph, film, video, picture or representation, portrait, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of obscene or sexually explicit conduct, where-

(i) the production of such visual depiction involves the use of a minor engaging in obscene or sexually explicit conduct; or

(ii) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in obscene or sexually explicit conduct; or

(iii) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in obscene or sexually explicit conduct, preparation, possession or distribution of any data stored on a computer disk or any other modern gadget.

Balochistan Child Protection Act, 2016

The Balochistan Child Protection Act, 2016 provides for the protection of vulnerable children from all forms of abuse, including sexual abuse, through the establishment of a Child Protection Commission and Child Protection Units in the districts responsible for the management of child protection cases. "Section 2(1)(w)" of the Act defines "sexual abuse and sexual exploitation" as:- (i) the inducement or coercion of a child to engage in any unlawful or psychologically harmful sexual activity; (ii) the use of children in commercial sexual exploitation; (iii) the use of children in audio or visual images of child sexual abuse; and (iv) child prostitution, sexual slavery, sexual exploitation in travel and tourism, trafficking (within and between countries) and sale of children for sexual purposes and forced marriage. Additionally, "Section 2(1)(t)" provides a detailed definition of mental violence against children. Subsection (vii) of the same section covers any psychological harassment of children by adults transmitted or carried out through the use of information technology, internet or cyber devices such as mobile phones. By extending the concept of harassment to include new technologies and use of children in audio or visual images of child sexual

abuse, the government of Balochistan has acknowledged the existence of online child abuse and the long-term consequences in lives of children[75] and allowed protective measures to be taken for child victims of such abuse as adequate and on the basis of their best interest.

Sindh Child Protection Authority Act, 2011

The Sindh Child Protection Authority Act, 2011 provides for the establishment of an Authority known as the Sindh Child Protection Authority for children in need of special protection measures. It is to monitor and coordinate child protection related issues at provincial and district levels and assist the Department of Social Welfare, Government of Sindh in establishing a case management and referral system to protect children from all forms of abuse, violence and exploitation. The Authority has established Child Protection Units and appointed Child Protection Officers to realise the objectives of this Act[76]. A child in need of special measures is a child who (i) is a victim of violence, abuse and exploitation, (ii) is subjected to physical and psychological violence, sexual abuse or commercial sexual exploitation, (iii) is forced into the worst forms of child labour, exploitative labour, or beggary, etc. Hence children who are victim of online abuse may benefit from protection services under this law.

Sindh Children Act, 1955

The Sindh Children Act, 1955, provides in "Section 56" that inducing and promoting seduction (including inducing immoral behaviour) or prostitution of girls below the age of 18 years shall be punishable with two years. "Section 57" deals with seduction or outrage of modesty. A person who engages in immoral conduct and seduces a girl under 18 years of age is liable to imprisonment for a term not exceeding two years and/or to a fine.

Punjab Destitute and Neglected Children Act, 2004

The Punjab Destitute and Neglected Children Act 2004 (PDNCA, 2004) provides for the rescue, protective custody, care, and rehabilitation of destitute and neglected children in the province of Punjab. "Section 3(k)" defines a destitute

75 "Legal and Technological Approaches to Tackle Online Child Abuse - Courting the Law." Courting the Law, 16 Mar. 2021, courtingthelaw.com/2021/03/16/commentary/legal-and-technological-approaches-to-tackle-online-child-abuse.

76 Child Protection Units District Level – Sindh Child Protection Authority. scpa.sindh.gov.pk/child-protection-units-district-level. Accessed 26 Nov. 2022.

and neglected child, and "Section 3(k)(v)" includes a child who is or may be abused or exploited for immoral or illegal purposes or unconscionable gain. To protect destitute and neglected children, the Act provides for the establishment of a Child Protection and Welfare Bureau, Child Protection Units, Child Protection Institutions and Child Protection Courts.

Punjab Protection of Women Against Violence Act, 2016

Similar to PDNCA 2004, this Act provides for the establishment of an effective system for the protection, relief and rehabilitation of women from violence in Punjab province, applicable to girls and women. "Section 2 (1r)" defines violence as "any offence committed against the human body of the aggrieved person, including abetment of an offence, domestic violence, sexual violence, psychological abuse, economic abuse, stalking or cybercrime". Implementation measures include a universal free helpline for aggrieved persons, the establishment of women's protection centres and shelters and a district committee for the protection of women, etc. Although the word cybercrime appears in the definition, it does not define exactly what cybercrime means, leaving the interpretation to law enforcement agencies.

The provincial governments of Sindh (2013)[77], Balochistan (2014)[78] and KP (2021)[79] have also enacted laws against domestic violence to institutionalise measures to prevent and protect women, children and other vulnerable persons from domestic violence. While these laws refer to sexual abuse and emotional and verbal abuse, they do not directly address or provide any protection against online sexual exploitation and abuse.

Due to the rapid development of information and communication technology, offenders today have more avenues and sophisticated tools to identify, target, groom and exploit children. Pakistan has done well in 2023 by amending the PECA 2016. The law now includes offences against OCSEA more comprehensively, but implementation and enforcement needs to be strengthened.

Although the Pakistani government has imposed a ban and blocked websites containing pornographic material, the content is easily accessible on new websites or through virtual private networks. Also, there is no legal provision that

77 The Domestic Violence (Prevention And Protection) Act, 2013

78 The Balochistan Domestic Violence (Prevention And Protection) Act, 2014

79 The Khyber Pakhtunkhwa Domestic Violence Against Women (Prevention And Protection) Act, 2021

exempts a child from any criminal responsibility for sharing CSAM, especially if forced to do so in an abusive situation. Consequently, children could be prevented from and/or or discouraged from reporting for fear of prosecution. Perpetrators could also theoretically exploit this loophole to blackmail children and take advantage of them for their own benefit.

The Punjab Protection of Women Against Violence Act, 2016, is neither child-centred nor child-sensitive. It is recommended to rely on child protection laws that cater to children only. Furthermore, the protections currently provided in provincial and federal child protection laws are too often based on the institutionalisation of victims, which is not in the best interests of the child. There is a need to strengthen efforts to reform alternative care in each province in line with international standards. Additionally, there is an urgent need to notify the outstanding child protection policies in all provinces of the country to guide and structure the state's response to OCSEA.

Judgement of Superior Courts

In recent years, superior courts of Pakistan have generated important jurisprudence on the issue of OCSEA.

Judgement of Islamabad High Court

Criminal Appeal No. 151/2020

MSK[80] versus The State

Justice Mohsin Akhtar Kayani of the Islamabad High Court authored the 24-page judgement while hearing an appeal against a conviction for child pornography. MSK, a male adult convict had appealed against his conviction by a lower court. In a January 2022 judgement, the Islamabad High Court upheld the conviction of the male adult, who had been sentenced to 14 years in jail and fined 1 million rupees.

The case against the accused was registered on August 25, 2019, on the complaint of the father of the child victim. According to the forensic report, 22,800 photos and 839 videos were recovered from the accused' s mobile phone. Most of the videos and photos show minor girls and boys who were groomed and sexually exploited and who the accused allegedly raped.

The Islamabad High Court has directed the federal government to take steps to increase the quantum of sentence on the charges of child pornography and issued guidelines to preserve the dignity of victims during the course of legal proceedings.

The court asked the federal government to amend the relevant section of the Prevention of Electronic Crimes Act, 2016, to increase the sentence from seven years to a maximum of 20 years, along with a fine of not less than one million rupees as awarded to the complainant in the said case.

80 Identity has been concealed due to "do no harm" principle, revealing the accused could inadvertently expose the victim, violating ethical and international obligations for their protection.

The IHC judgement provides guidance and states that in all cases of gender-based violence, courts must protect the rights of child victims of such cases by following the standards set out in international jurisprudence, adding that the victim must not be exposed to the accused or the courts and that his or her testimony must be recorded via a video link, if available.

The court suggested that the testimony can also be recorded by video conference, but that the child victim should not be in direct contact with the accused during the trial. The child should be placed in a conducive and protective environment, e.g. at home or in another separate facility if maintained by the government.

The court noted that the prosecution does not have to produce the victim in every case. Rather, the prosecution can prove its case on the basis of technical evidence of information technology, which falls under the modern devices permitted under the Qanun-e-Shahadat Order, 1984, and even under the international standards.

The order further states that the pornographic material shall not be exhibited in court and that the reports of the forensic laboratory or cybercrime expert shall be considered conclusive for the purpose of sentencing.

The IHC also directed the trial court to pass an order to remove all child pornography data which is accessible to anyone from any source and to direct the FIA and PTA to ensure that such data is not accessible in any information system to protect the dignity of the victim and the families. In addition to, the learned trial court should ensure that child pornography cases are heard in camera and that any outsiders unrelated to the case or additional court staff are excluded when taking the testimony of a child victim.

Announced on 14 January 2022

Judgement of the Supreme Court

Criminal Petition No. 1154 of 2021

KHK[81] versus The State and another

A two-member bench of the Supreme Court of Pakistan, comprising Justice Maqbool Baqar and Justice Syed Mazahar Ali Akbar, authored a three-page judgement stating that "child pornography is one of the major causes of sexual abuse of children and one of the major causes of devastation of society. It is a grave threat to the future and morality of children in this country."

The court rejected the bail application of the petitioner involved in spreading child pornography videos on social media. The charge against the petitioner is that he shared child pornography content on Facebook through his mobile phone. The Supreme Court of Pakistan held that people involved in heinous crimes against innocent children do not deserve relief. The court directed the trial court to expedite proceedings and conclude the case at the earliest.

The court noted that the petitioner was accused of distributing child pornography content through his Facebook profile and mobile device. After receiving the information from Facebook, the matter was investigated by the Federal Investigating Agency and after its completion, the FIR was registered and the petitioner was arrested.

The court remarked that the argument of the petitioner's lawyer that no affected party came forward was inadmissible. Although the offence with which the petitioner is charged does not fall under the prohibitory clause of "Section 497" of the Cr.P.C. and the maximum punishment for the same is seven years, given the nature of the charge, its impact on the society and the material collected so far merits the case to fall within the exception of granting bail when the offence falls within the non-prohibitory clause.

81 Identity has been concealed.

The court observed that "one of the most alarming social evils prevalent in society is child pornography. It has wreaked havoc in the society as it poses a great threat to the morals and future of children. One of the reasons for the increase in child abuse and rape cases is clearly due to child pornography. Concern about child sexual abuse and exploitation has been prevalent in society in the past as well. However, due to various factors, the severity and impact of child pornography is increasing at an alarming rate and this menace needs to be curbed with an iron hand".

Announced on 1st November 2021

Institutional Framework for Child Online Protection

COP is the concern of various ministries and departments, parliamentarians, National Human Rights Institutions (NHRIs), educators, civil society organisations, industry and parents and transcends national boundaries.

Federal Investigation Authority (FIA)

The Federal Investigation Agency is Pakistan's main national-level agency for investigating federal crimes. These include transnational organized crime, human trafficking, migrant smuggling, cybercrime, money laundering, terrorist financing, intellectual property rights, and electronic and physical bank fraud.

Cyber Crime Wing (CCW)

The Cyber Crime Wing (CCW) of the Federal Investigation Agency is guided by the PECA 2016, which addresses the growing threat of cybercrime. CCW was established in 2007 to identify and curb the phenomenon of technology misuse in society. The FIA receives direct complaints about cybercrimes and takes legal action against those who commit such crimes. The FIA received 84,764 complaints related to cybercrime in 2020 (FIA 2022). Most of the cases the FIA dealt with concern financial fraud. The FIA operates a cybercrime reporting helpline at 1991 and there is an online reporting portal at https://complaint.fia.gov.pk/. Fifteen (15) dedicated Cyber Crime Reporting Centres (CCRC) operate in six different zones of the country. Each circle or CCRC is headed by a Deputy Director who oversees the work of the CCRCs, forensic laboratories and the legal branch, and is supported by a team of investigators, prosecutors, cybercrime analysts, law officers, forensic experts and other support staff. CCW also has a Cyber Alert Service (CAS) to educate the public about cybercrime via SMS. It provides preventive tips on how to combat cybercrime.

The Unit Counter on Online Child Abuse (UCOCA) is a reporting centre set up by CCW as a specialised and dedicated unit to combat online child abuse within CCW Islamabad. UNOCA has designated focal persons in all 15 Cyber Crime Reporting Centres. It also acts as a focal contract for referrals from other countries on OCSEA. UNOCA is also engaged in processing and investigating high priority CyberTipline reports. Due to the high volume of CyberTipline reports, priority criteria are set by specialised investigators based on the CyberTipline reports.

INTERPOL's Child Sexual Exploitation (ICSE) database, is a tool used to advance child exploitation investigations through global information sharing by specialised investigators. FIA is in process to gain access of the database. INTERPOL has

completed the initial assessment in 2023 and an MoU has also been signed between the CCW of FIA and INTERPOL.

Police

The mandate of the police is to ensure the safety and welfare of children in their jurisdiction. This includes the prevention, investigation and prosecution of crimes and offences against children. With the recent amendments to the PECA 2016 in 2023, the police in Islamabad and all provinces can now take cognizance of cybercrimes under Section 30. This is an important development as the FIA is not present in all districts of Pakistan. However, the police are obliged to refer the matter to the FIA for a technical opinion and investigation.

Cyber Crime Investigation Unit
In response to the amendment of PECA 2016 in July 2023, Islamabad Police, which can now independently register cybercrime cases, opened its Cyber Crime Investigation Unit at F-6 Islamabad in January 2024 to combat cyber, aiming for a safe digital environment for residents.

Source: Islamabad Police

Pakistan Telecommunication Authority (PTA)

The Telecom Reorganisation Act, 1996 established the Pakistan Telecommunication Authority (PTA) as the regulatory authority for the telecommunications sector to regulate the establishment, operation and maintenance of telecommunications systems and the provision of telecommunications services. Under the PECA 2016, PTA has been mandated to block or remove unlawful content on the internet and ensure that the provision of telecommunication services is free from content that is harmful to children. PTA for facilitation in instant lodging complaints by public and Government organizations has developed state of art user-friendly complaints lodging mechanism E-Portal & CMS. Access of E-Portal has been given to government organizations including FIA for lodging complaints as per their mandate/areas of expertise whereas for lodging complaints related to Child Online Sexual Abuse "Child Abuse" category has been added in its Complaint Management System (CMS). Also provided emails to lodge complaints about nudity and pornographic content at content-complaint@pta.gov.pk and child pornography at reportchildporn@pta.gov.pk. In 2016, the Pakistan

Telecommunication Authority (PTA) had launched a crackdown on pornography on the orders of the Supreme Court and tasked internet service providers with a list of 429,343 domains to be blocked to control the distribution of pornographic material[82]. By December 2023, the PTA successfully blocked 983,089 pornographic or indecent content.

PTA regularly promotes awareness of the responsible use of technology and online safety for children through a variety of initiatives[83]. These include writing articles and publishing public service announcements in national and international newspapers and blogs, conducting digital literacy seminars and programmes for students, teachers and parents in educational institutions, participating in TV and radio programmes to raise awareness and disseminating safety guidelines for parents, teachers and students. PTA also regularly updates its website with recommendations and guidelines for parents, promoting the use of parental control software on mobile devices to prevent cybercrime and providing a list of recommended tools for this purpose[84].

In September 2023 PTA signed an MoU with TikTok in September 2023 to promote digital safety in government schools across Pakistan, using a multi-faceted approach. The initiative features comprehensive training programmes for teachers, parents, and students through a mix of workshops, seminars, webinars, and awareness videos. As part of the programme with TikTok, digital literacy trainings are being carried out in 100 schools across the country in the first phase. Also digital literacy books, guides and toolkits were developed for the training sessions and videos have been released emphasising the responsible use of social media, and mitigation of associated risks. In 2023, the trainings in Sindh and Gilgit-Baltistan were successfully completed.

In October 2023, PTA received recognition for its efforts under category "Enabling Child and Youth Safety Online" at the SAMENA Council International LEAD Award 2023 in the United Arab Emirates by the the SAMENA Telecom Council.

82 Pakistan Bans 429,343 Adult Websites. news.softpedia.com/news/pakistan-bans-429-343-adult-websites-499492.shtml. Accessed 29 Nov. 2022.

83 PTA. 23 Dec. 2022, pta.gov.pk.

84 Media Center | PTA. 22 June 2016, www.pta.gov.pk/en/media-center/single-media/parental-control-softwares--filters.

Keep Children Safe Online

PTA and UNICEF Pakistan joined forces in Islamabad on March 28, 2023, with a commitment to creating a secure online environment for children. This partnership focuses on preventing and reporting online child abuse incidents, fostering responsible internet use through awareness campaigns, and enhancing capacities among children, caregivers, and educators through capacity building programme. As part of the collaboration, PTA implemented various measures, including designating 1121 as a toll-free emergency helpline, contributing to UNICEF's Child Online Protection KAP survey part of UNICEF's global 'Disrupting Harm Programme', and compiling themes for awareness videos. The 'Keeping Children Safe Online' campaign, launched by PTA, emphasised parental controls through diverse media channels.

Source: PTA

The Ministry of Information Technology and Telecommunication

The Ministry of Information Technology and Telecommunication (MoITT) is the focal ministry of the Government of Pakistan responsible for planning, coordinating and directing programmes in the field of information technology and telecommunications. The Ministry has established a Cyber Governance Policy Committee (CGPC) to enforce policy initiatives related to cyber governance and security at the national level and to provide strategic oversight on national cyber security issues[85].

In 2021, the MoITT launched a "National Cyber Security Policy 2021" to address the incidents related to malicious use of information and communication technologies in cyberspace, which pose a serious financial and security threat to Pakistan[86]. The policy supports the creation of an internal framework in all public and private institutions for the protection of the cyber ecosystem, the security of national information systems and infrastructures, and the protection of all

85 NATIONAL CYBER SECURITY POLICY 2021. Ministry of Information Technology and Telecommunication, 2021.

86 Ibid.

national ICT infrastructures. A major gap in the National Cyber Security Policy 2021 is that the issue of COP and OCSEA is not addressed.

MoITT raises awareness through training for children, which includes cyber safety issues, and has launched a number of digital inclusion initiatives involving vulnerable groups such as girls, children and people with different abilities. Recognising that protecting children online is a global challenge, MoITT organised a successful "ITU-Pakistan Digital Inclusion Week: Meaningful ICT for All' from 12-13 December 2022 to promote a multi-stakeholder and inclusive approach to digital development. The event included discussions on key topics related to ICT, and two workshops were held on the topic of COP and Girls in ICT.

Child Protection Agencies (ICT and Provincial)

Each province and ICT have child protection agencies in accordance with their territorial laws to ensure that children have access to a functioning child protection system to protect children from abuse, violence, neglect, and exploitation. These include the Child Protection Institute in Islamabad, the Child Protection and Welfare Bureau in Punjab, the KP Child Protection and Welfare Commission in Khyber Pakhtunkhwa, the Sindh Child Protection Authority in Sindh and the Balochistan Child Protection Commission in Balochistan. Discussion with representatives of the Child Protection Institute and the Sindh Child Protection Bureau in December 2022 revealed that they had not been referred to any OCSEA case by the FIA, nor had they received any complaint from a victim. The Punjab Child Protection and Welfare Bureau does not provide services to the victims of online child abuse as the modus operandi of the Bureau is to first take the destitute and neglected children into its custody and only then provide services to these children.

UNICEF has supported child protection agencies across Pakistan to establish a child protection case management and referral system to provide support services to children, in need of protection including victims of OCSEA, or to refer them to the appropriate agencies so that victims receive appropriate care, protection and rehabilitation, in line with Pakistan's international obligations.

National Task Force on Prevention and Control of Cybercrimes against Children

The National Task Force on Prevention and Control of Cybercrimes against Children, set up by Wafaqi Mohtasib, played a very important role in developing strategies to counter OCSEA through two sub-committees: Legal Reforms and Awareness Raising. The Legal Reforms Sub-Committee took the lead in drafting the Criminal Laws Amendment Bill, 2022, which finally came into force in 2023. The Awareness Raising Sub-Committee implemented a strategy involving key stakeholders, education curricula inclusion and media campaigns by the PTA and others. However, the task force is currently dysfunctional and it is strongly recommended that it be reactivated.

Helplines

Helplines play a very important role where victims can lodge their complaints and get advice. The FIA runs a cybercrime helpline numbered "1991". The Ministry of Human Rights, which is a parent department of the Child Protection Institute, operates a helpline "1099" in ICT. The Child Protection & Welfare Bureau Punjab, the KP Child Protection & Welfare Commission and the Sindh Child Protection Authority operate a helpline with the same number "1121" in respective provinces. Importantly in 2023, the PTA has designated 1121 as a toll-free emergency helpline available to relevant provincial departments overseeing child protection, as well as those in AJ&K and GB.

Civil society organisations also run helplines, such as Digital Rights Foundation, which operates a free cyber harassment helpline "0800-39393", provide legal advice, psychological counselling and a referral system. Rozan operates a Rozan Counselling Helpline (RCHL) "0304-1111741" and offers counselling services where children and adults can call and share their concerns related to emotional, sexual and reproductive health, violence against women (VAW) and girls, and child sexual abuse (CSA).

National Human Rights Institutions (NHRIs)

NHRIs such as the National Commission on the Rights of Child (NCRC) and the National Commission for Human Rights (NCHR) have a national jurisdiction. Sub-national human rights institutions (SNHRIs) such as the Sindh Human Rights Commission (SHRC) focus on addressing human rights issues in the Sindh region. Both NHRIs and SNHRIs have a mandate to inquire and address complaints, including violations of children's rights.

National Commission on the Rights of Child (NCRC)

The NCRC is a monitoring and oversight body constituted under National Commission on the Rights of Child Act, 2017 having a national mandate for matters related to the promotion, protection and fulfilment of children's rights throughout Pakistan. The function of the Commission is to review existing or proposed laws and administrative instruments, conduct research, raise public awareness and advise on policy issues affecting children in Pakistan. The Commission investigates violations of the rights of the child and examines any factors that impede the enjoyment of the rights of the child, such as violence, abuse and exploitation, trafficking, torture, pornography and prostitution, and recommend appropriate remedial measures. Complaints can be made by telephone, email, through the website or through the Prime Minister Performance Delivery Unit.

The NCRC has been actively addressing the concern of COP, engaging key stakeholders in discussions, and advocating for robust measures to safeguard children from OCSEA across diverse platforms. This involves establishing a comprehensive knowledge base through research on COP and deploying awareness campaigns. In collaboration with PTA, the NCRC is set to conduct a Knowledge, Attitude, and Practices (KAP) survey under UNICEF's global 'Disrupting Harm Programme.' Additionally, there are plans to initiate training programmes tailored for parents, teachers, and children to enhance awareness and understanding of COP.

Cultivating Digital Competence of Youth and Parents

In 2023, Zindagi Trust, Meta, Pakistan Telecommunication Authority (PTA), Federal Investigation Agency (FIA) and the National Commission on the Rights of the Child (NCRC) collaborated to launch a digital campaign commemorating Children's Day. The aim of the initiative, called "Cultivating Digital Competence of Youth and Parents", was to promote youth safety in digital spaces and initiate a dialogue among youth and their parents about online safety, including reporting negative content such as online bullying, false information, hate speech and spam.

The collaborative digital campaign included video messages from students talking about safety tools such as privacy check up, locked profile, hidden words, supervision tools and how to deal with false information. This holistic approach, involving various stakeholders, industry safety partners and law enforcement agencies, emphasises the commitment to keeping young people safe online and promoting a responsible digital culture.

Source: Zindagi Trust

Ministry of Federal Education and Professional Training (MoFEPT)

The Ministry of Federal Education and Professional Training is the federal ministry mandated to develop national cohesion in educational policies and reforms, set educational standards, promote equity and cohesion, achieve universal literacy, coordinate academic assessment across Pakistan, etc. The National Curriculum Council (NCC) was established in 2015. The ministry is leading the development of a National Curriculum for Pakistan (formerly known as the Single National Curriculum) that covers four aspects of a quality curriculum, including standards, textbooks, teacher training and examination reforms. The curriculum focuses on life skills and pays some attention to child protection, and the MoFEPT plans to include cyber-bullying in the curriculum (ACTED 2022). Overall, the Ministry has a very important role to play and the curriculum must include the topic of COP, which should also address OCSEA and provide a reporting mechanism and training modules for teachers to teach students about safe and responsible online behaviour. The Ministry should also raise public awareness about the importance of online safety for children.

Federal Ministries and Provincial Departments

The Ministry of Interior is the administrative ministry of the FIA and the Islamabad Capital Territory police. It is primarily responsible for internal policies, the security of the state, the administration of the internal affairs of the state and the support of the government in territorial matters.

The Ministry of Human Rights at the federal level is the parent Ministry of the Child Protection Institute, mandated to establish and strengthen the necessary institutional mechanisms for the protection and promotion of human rights. The Ministry of Human Rights has launched a five-year National Action Plan on Human Rights and Business (2021-2026), which includes specific actions related to children's rights, but does not specifically address the issue of OCSEA.

Provincial departments such as Home Department, the Department of Social Affairs and the Department of Human Rights are important stakeholders in the administration of law enforcement and child protection agencies and have overarching roles and responsibilities.

eSafety Commissioner

The eSafety Commissioner (eSafety)[87] is Australia's independent online safety regulator with a shared goal of making the online experience safer and more positive for Australians. It is the world's first government agency dedicated to keeping people safe online. It began operations in 2015 as the Children's eSafety Commissioner and is now at the forefront of the fight against online risks and harms faced by both adults and children. The eSafety team consists of educators, investigators, lawyers, policy analysts, technology experts, digital specialists and other professionals.

UN Agencies

United Nations Children's Fund (UNICEF)

UNICEF is mandated by the United Nations General Assembly to advocate for the protection of children's rights, to help meet their basic needs and to expand their opportunities to reach their full potential. UNICEF advocates for online safety and advocates for necessary laws and regulations, and promotes the use

87 eSafety Commissioner. www.esafety.gov.au/homepage. Accessed 8 Dec. 2022.

of acceptable safety measures to protect children from violence, abuse and exploitation in the digital world88.

In Pakistan, UNICEF is playing a leading role in the fight against OCSEA. UNICEF is implementing a five-year country programme 2023-2028, in which COP is one of the priority areas. With a multifaceted approach, UNICEF has contributed significantly to the legislative reforms which led to amendments of the PECA 2016. In collaboration with key institutions such as the Pakistan Telecommunication Authority (PTA) and the National Commission on the Rights of Child (NCRC), UNICEF is involved in developing a knowledge base and raising awareness through different mediums. At provincial level, the organisation works with child protection authorities to establish a child protection system tor case management and referral system. UNICEF is also supporting the telecommunications company Telenor in Pakistan with capacity-building and awareness-raising initiatives to promote online safety among children.

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is the United Nations specialised agency for ICT. ITU supports all relevant stakeholders in their efforts to create a safe and empowering online environment for children and young people, enabling them to fully exercise their rights. COP is an initiative launched by the ITU in November 2008 as part of the Global Cybersecurity Agenda (GCA) to protect children worldwide from cyber threats[89]. ITU supports States in developing, adopting and implementing national frameworks and comprehensive strategies to COP, conducts research and provides awareness and capacity building for stakeholders[90].

International Criminal Police Organization (INTERPOL)

The International Criminal Police Organization, commonly known as INTERPOL, is an intergovernmental organisation with 195 member countries designed to facilitate the widest possible mutual assistance among all law enforcement agencies and to ensure that police services around the world can communicate securely with each other[91].

88 Protecting Children Online. 8 Feb. 2021, www.unicef.org/protection/violence-against-children-online.

89 ITU Global Cybersecurity Agenda and Child Online Protection (COP). www.unodc.org/documents/southeastasiaandpacific/2012/05/cyber-crime/ITU_Cybersecurity_COP_UNODC_Workshop.pdf. Accessed 3 Dec. 2022.

90 "ITU." ITU, www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx. Accessed 3 Dec. 2022.

91 INTERPOL | the International Criminal Police Organization. www.interpol.int/en. Accessed 4 Dec. 2022.

INTERPOL's Child Sexual Exploitation Database

INTERPOL's child sexual exploitation image and video database is an intelligence and investigative tool that enables specialised investigators to share data on child sexual abuse cases[92]. By analysing the digital, visual and audio content of photos and videos using image and video matching software, investigators can instantly make connections between victims, abusers and locations. The database avoids duplication and saves valuable time by letting investigators know if a series of images has already been discovered or identified in another country, or if it has similar characteristics to other images. It also allows specialised investigators from more than 68 countries to exchange information and share data with their colleagues around the world. This database contains more than 4.3 million images and videos and has helped identify more than 30,000 victims worldwide (Interpol 2022).

Civil Society Organisations

NGOs, INGOs and the media play a very important role in promoting COP and children's safety agenda. They are not only watchdogs, but also raise awareness about the harms and dangers of ICT on children. The Digital Rights Foundation, for example, is a research-based NGO that focuses on ICT to support human rights, digital governance and democratic processes. Sahil monitors child sexual abuse cases, including victims of OCSEA. Zingadi Trust conducts digital safety workshops in schools and has also organised seminars to raise awareness on safe internet use. There are other examples of good work being done by different CSOs in Pakistan[93].

ECPAT is one of the leading INGOs working internationally on COP. Other organisations include Child Rights Connect, Save the Children, International Centre for Missing and Exploited Children (ICMEC), Terre Des Hommes, Plan International, etc.

92 Ibid.

93 To See which CSO or institution could provide services to child victims of online abuse, in which province, you may also refer to: https://victimservicedirectory.org

WeProtect Global Alliance[94]

The WePROTECT Global Alliance is an international alliance that works globally to end the sexual exploitation of children online. The Alliance is registered as an independent organisation. It brings together governments, law enforcement agencies, civil society organisations and private sector companies to share information and coordinate efforts to identify and protect victims and prosecute perpetrators. A Model National Response (MNR) developed by the Alliance helps countries establish and implement a coordinated national response preventing and tackling online child sexual exploitation.

WeProtect Model National Response
WeProtect Global Alliance Model National Response (MNR) provides a comprehensive blueprint for effectively addressing online child sexual exploitation and abuse at the national level.

The Framework outlines the priority areas of intervention for nations, focusing on the following:

POLICY AND GOVERNANCE
Highest level national commitment to child sexual exploitation and abuse prevention and response

CRIMINAL JUSTICE
Effective and successful child sexual exploitation and abuse investigations, convictions and offender management

VICTIM
Appropriate support services for children and young people

SOCIETAL
Prevention of child sexual exploitation and abuse

INDUSTRY
Industry engaged in developing solutions to prevent and tackle child sexual exploitation and abuse

COMMUNICATION AND MEDIA
Awareness raised among the public, professionals and policymakers

(See Annexure-1 for the Full Framework)

94 WeProtect Global Alliance. https://www.weprotect.org/

South Asia Initiative to End Violence Against Children (SAIEVAC)[95]

Pakistan is a member of the South Asia Initiative to End Violence Against Children (SAIEVAC), a regional network of government agencies, civil society organisations and other stakeholders working to end all forms of violence against children in South Asia, including child sexual abuse and exploitation.

Private Companies

There are a number of companies providing information and communication technology services, including mobile operators, internet service providers, telecommunication companies, user-generated content and social media providers, data hosting companies, etc., that play an important role in the field of COP.

Telenor, one of the leading telecommunications companies in Pakistan, partnered with UNICEF in 2022 to promote safe and responsible internet use among children, caregivers and educators through awareness raising and capacity building[96] and plans to train 750000 individuals using a hybrid training module.

In 2021, Apple had announced a plan to scan photos stored by users in iCloud for CSAM[97]. The tool was meant to be privacy-preserving and allow the company to flag potentially problematic and abusive content without revealing anything else. But it soon came under criticism because the surveillance capability itself could be abused to undermine the privacy and security of iCloud users around the world. In early September 2021, Apple announced that it would pause the rollout of the feature. However, in December 2022, company says it is discontinuing the CSAM detection tool for iCloud photos in response to the feedback and advice it has received. Instead, Apple is now focusing its anti-CSAM efforts and investments on its "Communication Safety" features to stop child exploitation before it happens or becomes entrenched, and reduce the creation of new CSAM.

95 South Asia Initiative to End Violence Against Chidlren https://saievac.org/

96 Telenor Pakistan and UNICEF Partner to Strengthen Child Online Protection - Telenor Pakistan. 3 Nov. 2022, www.telenor.com.pk/news-event/telenor-pakistan-and-unicef-partner-to-strengthen-child-online-protection.

97 Nast, Condé, and @wired. Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next. 7 Dec. 2022, www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages.

Facebook, Google, Microsoft, Yahoo, Tiktok, etc. have blocked hundreds of keywords related to child sexual abuse material on their platforms[98]. Social networks, messaging platforms and search engines such as WhatsApp, Facebook, Twitter, Instagram, Flickr, MySpace and Google block and report offensive and abusive material through filters, privacy settings and complaint mechanisms. Since 2011, many social media platforms have used Photo DNA technology to scan every uploaded photo and control the spread of child sexual abuse material. Search engines such as Google, Yahoo and Bing also block searches for illegal material to control the distribution of such videos, photos and content, and use splash pages to warn users when they are about to access illegal or harmful content.

Social media platform X (formerly Twitter) is set to establish a moderation office in Texas in 2024, emphasizing the fight against content related to child sexual abuse[99]. The "Trust and Safety Center of Excellence" in Austin aims to recruit 100 content moderators, with a primary focus on eradicating child sexual exploitation content and enforcing platform rules. Although X does not have a specific line of business dedicated to children, the company, is planning to preventing offenders from utilizing the platform for the distribution or engagement of CSAM.

98 Mandavia, Megha. "Facebook, Google Blocking Search Words Linked to Child Porn." The Economic Times, economictimes.indiatimes.com/tech/internet/facebook-google-blocking-search-words-linked-to-child-porn/articleshow/67186564.cms. Accessed 4 Dec. 2022.

99 A. (2024, January 29). *X to open new office to combat child porn*. DAWN.COM. https://www.dawn.com/news/1809477

Challenges and Issues

Given the dramatic increase in the number of children using information and communication technologies, there are a large number of children who are at risk from technology facilitated violence against children. This requires a good understanding of the issues involved and timely solutions to address OCSEA. This section discusses a number of issues and challenges that require the attention of key stakeholders.

Generational and Knowledge Gap between Parents/Adult Caregivers and Children

The generational gap in internet use between children and parents/adult caregivers is very large. The biggest challenge with the increase in online activity is that children are participating in things online and doing things at home that many parents/adult caregivers do not know about or are not familiar with. There are many new games, apps, websites, social networks, etc. There is concern that increasing access to internet and use of social media is having harmful effects[100]. This becomes serious when parents are no longer able to understand their children's experiences or protect and support them effectively.

Lack of Literacy and Digital Gender Gap

Another significant challenge in addressing OCSEA is the lack of literacy, including digital literacy, particularly among women. The digital gender gap makes it difficult for parents and adult caregivers in monitoring their children's online activities and providing adequate support. According to a report by the World Economic Forum[101], the digital gender gap refers to the disparity in access to and usage of digital technologies between men and women. In Pakistan, this gap persists, with women having limited access to new technologies and fewer opportunities for digital skill development. As a result, parents and caregivers, especially women, may struggle to understand and navigate online platforms and tools, making it challenging to effectively monitor and protect children from online risks and exploitation.

Covid-19 Increased the Risks of Children's Addiction to ICT

Children spent hours at home in front of the screens of tablets, smart phones and computers playing electronic games during covid-19 pandemic. There is no doubt that the sudden change in children's lifestyle during the Covid-19

pandemic has led to serious consequences and the addiction of ICT[102]. Moreover, many schools and parents in Pakistan had to make arrangements for online classes where children sat in front of screens for hours. As a result, the screen time of school children also increased. While parents were busy with their work and other activities, it was not possible for parents to monitor children's activities during classes, leaving children more vulnerable to OCSEA.

Changing Patterns of Usage of Technology

The fact that many activities that were formerly performed on fixed computers are now frequently performed on mobile devices with internet access further limits parents' ability to protect their children[103]. Parents are less able to supervise their children's activities, implement filtering or blocking measures, or regulate the level of Internet access when children have access to such phones, which is the case for a growing number of kids. This changing pattern of use presents fundamentally different challenges that need to be considered when introducing protection or prevention strategies[104].

Cultural Barriers

In a traditional society like Pakistan's, parents and teachers find it difficult to talk about issues such as sex, molestation, and sexual abuse of children because the subject is often tainted with shame and stigma and considered inappropriate. As a result of their silence, children remain vulnerable to OCSEA because they do not know how to cope and react when the perpetrators approach them. It is a common concern that children do not report cases of OCSEA because they are afraid of being blamed or not taken seriously. This is a serious problem that needs to be addressed to ensure that children receive the support and protection they need, instead of facing secondary victimisation. The other dimension of the cultural barrier is that many parents and family elders cannot come to terms with the fact that technology is eroding the traditional boundaries of the family. A father shot dead his 18-year-old daughter in Vano Ghari village in Sardaryab, Khyber-Pakhtunkhwa, after a video of her dancing went viral on social media[105].

102 Covid-19 Pandemic and Its Impact on Increasing the Risks of Children's Addiction to Electronic Games From a Social Work Perspective. 1 Dec. 2021, www.sciencedirect.com/science/article/pii/S2405844021026062.

103 Child Safety Online: Global Challenges and Strategies. UNICEF, 2011.

104 Ibid.

105 The Current. 24 Jan. 2023, thecurrent.pk/father-kills-18-year-old-daughter-after-her-dance-video-

So when there is no communication between children and parents and no proper supervision, children can engage in activities that are unacceptable to many in the family.

Unaware of the Harms and Risk sharing Personal Information Online

Clear boundaries used in the physical world to delineate different aspects or contexts of life do not necessarily exist or function in the same way online[106]. Research from around the world has found that young people often feel safer disclosing highly sensitive personal information or engaging in sexualised behaviour online than they do offline. Online platforms, on the other hand, whether chat rooms, blogs, online games or social networks, deconstruct the traditional boundaries of privacy. Children conversing in the privacy of their own bedrooms may knowingly or unknowingly expose themselves to an unknown global audience, which can increase the risk of harm and exploitation[107].

Lack of Focus by Schools on Teaching Digital Skills

In most schools in Pakistan, computer education is part of the curriculum, but children are not adequately educated about the dangers and risks of ICT use and are not taught about how to protect themselves offline and online. Many teachers also do not have sufficient knowledge and skills. Digital skills for child safety are critical for ensuring that children are equipped to navigate the digital world safely and responsibly. By teaching children these skills, they can help children to protect them from online harm and empower them to make the most of the opportunities that technology provides. It is also worth noting that while the formal education system makes it possible to reach school-going children, not all children in Pakistan have access to formal education, but many of them now have access to mobile phones, and remain vulnerable.

Anonymity of Users

Many of the risks children face online stem from the fact that they cannot verify their age and that users remain anonymous on digital platforms. This causes two major problems: first, children interact freely with users of all ages without being

goes-viral.

106 Child Safety Online: Global Challenges and Strategies Technical Report. UNICEF, 2012.

107 Ibid.

aware of the age difference between them and the people they interact with. Secondly, minors may have unrestricted access to content that is inappropriate for their age, such as pornographic or violent content. UK regulator Ofcom warned in October that adult websites with explicit content are not doing enough to protect children[108]. Few bother to do more than ask visitors to self-declare that they are over 18.

Detection of Technology Facilitated Violence against Children is Difficult

Moreover, violence against children perpetrated through the use of technology is more difficult to detect and combat than traditional forms of violence against children. It is challenging for law enforcement agencies to detect suspicious activities, identify perpetrators, investigate and prosecute illegal activities against children when these activities are committed using ICT. This is because technological advances allow internet users to surf anonymously on Tor network-based websites and conduct electronic transactions with virtual currencies that cannot be easily regulated by existing laws and regulations.

Additionally, distributors and consumers of the CSAM have developed sophisticated, cross-platform strategies to avoid detection. They often use the most popular platforms to find a community of child abusers to whom they can offer the material in encrypted language. They share links on platforms to material that is visible to everyone, using encrypted language to evade the companies' detection tools. They then direct interested consumers to more private channels where they can access the material, often via encrypted messaging apps or poorly monitored file-sharing services.

Limited Research and Evidence on OCSEA

Available research on OCSEA is limited in Pakistan. There appears to be no effort to collect systematic, regular and comprehensive data on the magnitude and nature of online and offline child sexual abuse, taking into account the new forms of online threats that children face today. Existing data available from FIA does not reflect the full scale of the problem, as it only focuses on cases reported online.

108 Hern, Alex. "Porn Sites Are Not Doing Enough to Protect Children, Warns Ofcom." The Guardian, 20 Oct. 2022, www.theguardian.com/technology/2022/oct/20/porn-sites-not-doing-enough-protect-children-ofcom.

Inconsistent Application of Security Protocols by Technology Companies

The standards and security protocols of different technology companies are often applied differently. There are new platforms, start-ups and new technologies, for example social gaming and Mataverse. The most important goal for these new platforms is to grow and gain a market foothold. The same applies to new businesses. To achieve this, companies try to attract as many users as possible to their platforms. Therefore, the entry barriers to join the platform are kept as low as possible to ensure a smooth sign-up process. If too many hurdles are added, users will find the cost of trying with uncertain satisfaction levels too high and simply go elsewhere. For this reason, they keep the enrolment process as smooth as possible and forgo pre-screening measures such as parental consent assurances in the background.

Age ratings for apps are inconsistently enforced

The findings of Reviewing the Enforcement of App Age Ratings in Apple's App Shop and Google Play, conducted by the Canadian Centre for Child Protection (C3P) as part of an analysis of child safety in the two largest mobile app stores, show that app stores are not delivering on their promises to keep young users safe. Age ratings for apps are inconsistently enforced. For example, on Apple's App Store, a 13-year-old can download apps with a 17+ age rating simply by clicking on a pop-up window to confirm they are 17+, even though Apple knows the user is 13 based on the age entered in their account. YouTube is rated 17+ on Apple, 13+ ("Teen") on Google Play and 13+ in YouTube's terms of service. Both app stores have not been transparent about how they set age ratings for apps, and the content of is inconsistent. For example, in Apple's App Store has several content descriptions, including "Infrequent/mild sexual content and nudity" and "frequent/intense mature/suggestive themes", while Google Play's content descriptors for YouTube are "user interact" and "digital purchases"

Canadian Centre for Child Protection (2023)

Self Regulation and Voluntarily Measures are not Sufficient

Measures to prevent and detect harmful and explicit content have largely been left to the self-regulation of digital service and platform providers. Voluntary measures

to combat OCSEA are fraught with difficulties. Removal of content by social media is usually the result of either an automatic filter or users of a service flagging content they deem inappropriate. Shortcomings in the definition of 'harmful content' have led to inconsistent application of terms of use and standards by digital service and platform providers within and between countries[109]. In some cases, human moderators are used to decide whether something should be removed, even though it would be virtually impossible for them to go through every single post on a social network[110]. It may also happen that a moderator cannot determine whether or not a flagged CSAM photo is actually a minor or an adult. In this case, moderators may assume that the subject is an adult[111].

The Centre for Digital Democracy (CDD) finds that social media platforms are still not doing enough to protect children, despite a flood of new safety features in its latest report released in November 2022[112]. The CDD researchers have analysed the strategies of the technology industry. These companies have introduced a flood of new tools, default navigation systems and AI software to improve protection against child sexual abuse material, problematic content and disinformation. However, technology platforms have been careful to ensure that the new safety systems do not significantly interfere with advertising practices and business models that target the lucrative youth demographic. The report concludes that security measures are fragmented and inconsistent. Most of the operations within these social media companies remain hidden from the public, leaving many unanswered questions about how the various safety protocols and youth-friendly policies actually work.

No Role of Child Protection Agencies

Child protection agencies exist in all provinces of Pakistan and are mandated

109 Crawford, Kate & Gillespie, Tarleton. (2014). What Is a Flag For? Social Media Reporting Tools and the Vocabulary of Complaint. New Media & Society. 18. 10.1177/1461444814543163.

110 Facebook Moderators 'Err on the Side of an Adult' When Uncertain of Age in Possible Abuse Photos. 1 Apr. 2022, www.theverge.com/2022/3/31/23005576/facebook-content-moderators-child-sexual-abuse-material-csam-policy.

111 Ibid.

112 Kathryn C. Montgomery, Kathryn C. Montgomery, et al. Social Media Platform Safeguards for Whom? Centre for Digital Demoracy, 2022.

to respond to and provide support to children who are at risk or in need of protection. Child protection agencies have a very important role to play especially when children come into contact with the law. From discussions with various child protection agencies, it appears that unfortunately there is limited liaison and coordination with the CCW FIA when it comes to cases of OCSEA and that the issue of COP is not yet on their radar. Child protection agencies lack knowledge regarding this issue of online safety, are also significantly understaffed, and face budgetary constraints that deeply affect their work. Many times, they are dependent on support from development partners.

Poor Awareness and Understanding of OCSEA among Key Stakeholders

Awareness and understanding of the scale and severity of the OCSEA problem remains limited among key stakeholders. The main reason for this is that it is a new area for FIA and child protection workforce in Pakistan. Many people are not at all familiar with the issue, have a poor understanding of the legal framework and do not know how to prevent and respond and what role to play in combating OCSEA. This also applies to lawyers, prosecutors, and judges. The subject is technical and one-off training sessions are not enough. A full fledge multi-sectoral capacity-building program is required.

Limited Effectiveness of Helplines

In addition to the "1991" FIA cybercrime reporting helpline, there are a number of other helplines in Islamabad Capital Territory and provinces. The findings show that helplines are poorly linked to the FIA and other referral systems, making it very difficult for them to effectively help victims of OCSEA. Moreover, helplines are often understaffed, have limited access to trained staff and lack the financial resources to be effective.

Mandatory Requirement for Physical Verification

One significant challenge is the mandatory need for physical verification. Although there is an online option to initiate the registration of the complaint, individuals wishing to pursue the complaint need to visit the FIA office in person to have it verified (FIA 2023). This requirement discourages many people from pursuing their complaint. Compounding the issue is the FIA offices have limited geographical coverage, making the process cumbersome for complainants who have to travel outside their city to lodge a complaint. This discourages reporting

of incidents at early stages. Efforts should be made to simplify the process of registering complaints and remove barriers that may prevent individuals from seeking justice for online offences of OCSEA.

Lack of Reporting by Victims and/or Families

Discussions with FIA and civil society organisations revealed a general reluctance to report OCSEA. One of the reasons for this reluctance is the shame and stigma associated with child sexual abuse, fear of retribution by the perpetrator, parents, caregivers, family and community members. Many victims and their families prefer to remain silent (FIA 2022). Other reasons cited are the mandatory requirement to verify complaints, lack of confidence in the effectiveness of the reporting system and in the criminal justice system (Digital Rights Foundation 2022), as investigation, and prosecution of child sexual exploitation and abuse cases risks re-victimisation of children if it relies heavily on child victims and their testimony in court and participation in criminal proceedings. This leads to cases not being reported or charges being withdrawn and statements recanted.

> The FIA shared with the NCRC details of a case in which a man was arrested for financial fraud (FIA 2022). During a phone search, it was found that the arrested man had repeatedly sexually abused his minor relative and made videos of her. Further investigation revealed that the man had sold these videos on the internet. However, when the case was discussed with the victim's family, they did not want to press charges as this would bring shame to the family.

Number of NCMEC Cases Investigated is Low

Electronic service providers (Facebook, Google, etc.) refer OCSEA cases to NCMEC and NCMEC forwards these cases to the relevant law enforcement agency for necessary action.

Country	# of Reports from NCMEC (2019)	# of Reports from NCMEC (2020)	% Increase in Reports from NCMEC	# of Reports Investigated by Law Enforcement	# of Reports from NCMEC to Investigated Cases per 100,000
Pakistan	1,158,390	1,288,513	11.23	103	8
India	1,987,430	2,725,518	37.14	1,102	40
Philippines	801,272	1,339,597	67.18	160	20

Source: CyberTipline

The table illustrates the dramatically low number of OCSEA cases investigated per year in Pakistan, India and the Philippines. In all these three countries, a total of 2,380 cases of OCSEA were investigated per 100,000 reports submitted by NCMEC. This basically shows that a significant number of NCMEC reports on OCSEA seem to disappear into an unregulated, unlawful and uninvestigated black hole. Additionally, each country applies its own national laws when assessing the reported content. It also shows that the FIA is probably unable to cope with the sheer volume of reports it receives.

According to the FIA, apart from the number of cases it receives from the NCMEC, there are also real complications in investigations. For example, when the ECP reports a case to the NCMEC, in many cases the content is removed from the website. The users who uploaded and shared the content are often blocked. This is done from a fake account that is already closed. It is extremely difficult to track down the person. Another problem is that in most cases there is no complainant and it is difficult to find a victim, who in most cases reside outside Pakistan. FIA is in process to gain access to INTERPOL's ICSE database, which will be useful in investigating OCSEA cases (FIA 2024).

Capacity Issues of Law Enforcement Agencies (FIA and Police)

The first problem is that the FIA has its offices in 15 cities of Pakistan. When cases are reported from outside these cities, it is not very easy for the FIA to act immediately and effectively because of the limited number of officials. The staff is already overburdened with the ever-increasing number of cases. The second problem is that many investigators do not have the necessary expertise or experience to deal with child-sensitive investigations (Digital Rights Foundation, 2022). Technology is constantly evolving, and investigating electronic crimes is a challenge. Therefore, there is a need to strengthen the investigative units under CCW of the FIA, which should provide regular training and orientation sessions for FIA staff and other officials involved in investigations. It is also important to address the issue of vicarious trauma experienced by FIA personnel, which is an important aspect of law enforcement officers' mental health.

Although recent legislative amendments to the PECA 2016 empower the police to take cognizance of OCSEA cases, there is a major challenge – a lack of adequate manpower and expertise within the police force. To effectively combat OCSEA, it is imperative that the police invest significantly in developing the personnel and expertise required to thoroughly investigate and prosecute in this critical area of COP.

Gaps in Laws Enforcement

It is important to note that Pakistan has made significant progress in criminalising various forms of OCSEA, however there are serious gaps in the enforcement of the law. Viewing child pornography is not expressly punishable under law. The deficits lie in systemic challenges with overall weak child protection systems and institutional structures that struggle to effectively coordinate responses to OCSEA. Furthermore, the development of deepfake technology is an example of the need for legislation to constantly evolve as the tools people use to create and share CSAM change.

Lack of a Child and Gender-Sensitive Justice System

A child and gender-sensitive justice system is one that is specifically tailored to the unique needs and perspectives of children, who may have different experiences than adults. Various laws in Pakistan provide for exclusive courts for children in contact and conflict with the law. However only few children's courts are notified and are not properly equipped to provide effective support and justice to children in accordance with Pakistani laws and acceptable international standards. These include, for example, court procedures that are too complex

for children, separate hearings, a lack of specialised resources for child victims and witnesses, and a general lack of sensitivity to the special needs of children in the justice process. The recent amendment to the Qanoon-e-Shahadat Order, 1984[113] has allowed admissibility of testimonies taken by the court using modern equipment or techniques, but it remains to be seen how and when the court system will actually enforce this. Overall, a system needs to be created that provides child victims with access to justice that respects and effectively protects children's rights. Whilst very positive and successful examples of specifc child courts have been piloted in the country, such models are yet to be consolidated and upscaled. Furthermore, it is necessary to address the issue of vicarious trauma experienced by justice actors involved in child-sensitive cases. They are significantly impacted when confronted with distressing cases of OCSEA without adequate psychological support.

Issues with Jurisdictions and Multiple Legal Systems

Dealing with OCSEA cases is challenging because they are rarely confined to one country or one area to which a particular legal system applies. Determining whether a crime has been committed inside or outside Pakistan's territory is not straightforward. In complex cases, there may be multiple perpetrators, multiple victims, and multiple platforms, all located in different countries. Crimes, by their very nature, are committed across numerous jurisdictions. This makes the investigation and prosecution of OCSEA crimes particularly challenging, as it raises the question of which country's laws will be applied to hold perpetrators accountable and what mechanisms should be used to prosecute them. Inconsistencies at both international and national levels in the definitions of OCSEA and the application of terms of use of service providers and platforms have made it difficult to identify and prosecute perpetrators. While some international and national laws and mechanisms exist to establish jurisdiction, the various forms of OCSEA would need to be clearly defined as crimes at the national level and the countries concerned would need to cooperate with each other in prosecuting OCSEA-related crimes.

113 The Criminal Laws (Amendment) Act, 2023

Recommendations

The threat that advances in information and communication technologies pose to the safety and protection of children is increasingly being recognised. The Government of Pakistan has taken some steps to address the issue, but much more is needed given the magnitude of the problem. Addressing the multidimensional threat posed by technology requires a holistic approach that includes adopting policies and enforcing laws, as well as raising awareness, building capacity, strengthening child protection systems in line with international standards and forming partnerships with CSOs, as well as private, national and international companies.

Children

- Giving children the tools to protect themselves from the dangers of technology and become aware of their responsibilities is probably the most effective way of safeguarding children's rights in digital world. Some steps that can be taken are: educate children about online risks and potential dangers, equip them to report suspicious behaviours and cases of OCSEA, keep personal information private, use privacy settings, talk to trusted adults, etc. Children can also help raise awareness of the problem of OCSEA by passing on information to their peers and encouraging them to be vigilant and take action to protect themselves.

Parents/Guardians/Caregivers

- Parents and guardians need to first encourage open and honest communication with their children and be a supportive resource when they come forward with concerns about OCSEA. It is the responsibility of parents to educate their children about the dangers of OCSEA and to make them understand that it is never their fault if they become a victim, and that as parents, guardians, caregivers, they will always be there to support, guide and protect their child.

- One of the best-known tools that can help parents keep their children safe online is the use of parental controls, an umbrella term for a variety of different applications and settings that parents can use to monitor and restrict their children's digital activities. Parental control tools allow parents to proactively protect their children.

Nayatel, an ISP, offers free parental control to its customers in Pakistan. The interface helps parents set up parental lock like an alarm on your smartphone[114]. There is an additional Safe Web service that restricts access to harmful websites and content for children for an additional fee[115].

114 Nayatel Parental Locking - Lock Your Internet Anytime. nayatel.com/parental-locking. Accessed 14 Dec. 2022.

115 Safe Web - Nayatel. nayatel.com/safe-web. Accessed 14 Dec. 2022.

- It is important that parents limit and control the time their children spend on screens. The more time children spend on screens, the unhealthier it is and the more prone they are to OCSEA. Parents also need to set ground rules for online behaviour, set expectations and discuss different forms of OCSEA with children. This helps to identify OCSEA and encourage them to report it.

Educators

- Educators play a crucial role in preventing and raising awareness of COP in schools and educational institutions. They have the opportunity to provide guidance, support and resources to students and parents on how to use the digital world safely.
- Integrate COP education into the curriculum to ensure students receive age-appropriate information about online risks and safety measures.
- Provide training and workshops for teachers on recognising signs of OCSEA in students and how to respond effectively.
- Introduce clear child protection policies and guidelines for online behaviour and use in schools, including protocols for reporting OCSEA incidents.
- Creating a supportive environment where students feel comfortable talking about their online experiences and seeking help when needed.

Electronic Service Providers

- The technology industry has a critical role to play in establishing the foundations for safer and more secure use of internet based services and other technologies – for today's children and future generations. Businesses must put protecting children at the heart of their work, paying special attention and putting systems in place to address violations of children's rights.

> "Putting a duty on App Stores to identify children and prevent them from downloading apps where there is a high risk of grooming will focus company minds on ensuring the problem is tackled on their platforms."
>
> Andy Burrows, Head of Child Safety Online
> The National Society for the Prevention of Cruelty to Children

- There is a need for the development of innovative technological solutions that improve existing approaches to preventing and combating OCSEA or enable the development of new approaches. If ESP proactively shares its unique knowledge and offers technology-based solutions to relevant stakeholders, this will strengthen collective efforts to reduce OCSEA.

- All platforms operating from Pakistan must make flagging, blocking and reporting mechanisms within online platforms clear and accessible to children. These mechanisms should be child-friendly and explicitly outline what children can expect after submitting a report. Platforms and service providers must demonstrate transparency and accountability in the way they respond to children's reports in a timely manner, take appropriate action within their terms of use, and report to CCW FIA.

An example of a private initiative to detect online child sexual abuse material is the technology developed by Netclean, which works similar to an anti-virus programme[116]. The software can be installed on any computer or network and will detect any images and videos that law enforcement agencies have classified as child sexual abuse material.

- Technology companies should consider proactively detecting and eliminating CSAM and identifying grooming attempts and live-streamed CSAM by using technology tools such as PhotoDNA and API Arachnid. Age-protection solutions can help protect children from these harms by providing platforms with the information they need to enforce age-based rules and policies. Currently, there are two main methods to determine a user's age: age verification and age estimation. Age verification describes procedures that validate the user's age using official documents (such as a government-issued ID or credit card information) or a biometric face. Age estimation, on the other hand, is the process of predicting a person's age based on various factors such as facial features, voice and behavioural patterns. Age estimation algorithms use machine learning and artificial intelligence techniques to analyse data and make predictions about a person's age.

116 "About." NetClean, www.netclean.com/about. Accessed 15 Dec. 2022.

In UK, Microsoft has teamed up with Child Exploitation and Online Protection Centre (CEOP) to install a red panic button on Internet browsers for users[117]. When a user clicks on the panic button, a computer programme sends a message to the National Crime Police and calls up a tip page to report online sexual abuse. Microsoft provides parents with a range of information to educate their children about internet safety and discourage them from communicating online with strangers.

European Commission has developed a blocking mechanism for ISPs called the Child Sexual Abuse Anti-Distribution Filter, which is currently used by ISPs in Denmark, Finland, Italy, Malta, Norway and Sweden[118].

- The FIA can work with ISPs to set up alert mechanisms when child abuse content is accessed through the search engines that enable the dark web. The mechanisms should also have programmes that detect the software and search engines used to access the Dark Web. In this way, the explicit content cannot only be blocked but also help in apprehending the perpetrators.

Government and Law Enforcement Agencies

- It is strongly recommended that the CCW of the FIA and Police be strengthened with additional human, budgetary, technical and financial support. There is a need to invest in research and additional equipment and tools to detect, evaluate and analyse child sexual abuse material. Currently, the FIA does not have sufficient staff, experts, and tools to collect and examine digital evidence at sufficient speed for the CCW to conduct proactive and victim-centred investigations and to cooperate nationally and internationally. The government should provide FIA the state-of-the-art equipment, and continuous training on new tools and emerging technologies is also essential.

117 "Microsoft, CEOP Adds Panic Button to IE8 to Fight Online Child Abuse." ZDNET, www.zdnet.com/article/microsoft-ceop-adds-panic-button-to-ie8-to-fight-online-child-abuse. Accessed 15 Dec. 2022.

118 "Legal and Technological Approaches to Tackle Online Child Abuse - Courting the Law." Courting the Law, 16 Mar. 2021, courtingthelaw.com/2021/03/16/commentary/legal-and-technological-approaches-to-tackle-online-child-abuse.

- Psychological support to tackle vicarious trauma to concerned LEAs also required to ensure the mental well-being of officers and enhance their ability to effectively investigate and address cases of child exploitation and abuse.

- The government needs to further strengthen the 1991 helpline established by CCW of FIA by providing them with more professional capacity, adequate resources, and better accessibility to children through online technologies such as social media, online chat etc. It should also ensure better coordination with all other helplines at national and federal levels and be linked to Police and the child protection system. The helpline should be widely publicized, including in schools and other public places accessed by children: hospitals, transport hubs, markets, etc.

- It is recommended that the CCW FIA should use a child protection case management and referral system (CP-CMRS) for investigation, information sharing and general co-operation in the handling of OCSEA cases.

- The overall response to children in need of protection must focus on child protection agencies and authorities rather than law enforcement alone. Direct contact with children and families should be led by trained professionals, as law enforcement agencies are not experts in children's rights and child protection. There is a need to strengthen child protection agencies with staff and budgetary resources. Close cooperation of child protection workforce with law enforcement agencies will actually reduce the burden of FIA.

- Capacity building trainings on COP should be provided to CCW FIA, Police, child protection officers and social workers. These trainings may include understanding the issues, recognising child sexual abuse and exploitation, investigating and collecting evidence of cybercrimes against children, identifying and interviewing child victims, referral and coordination, and providing psychosocial support to victims.

- Conduct training for justice professionals, including prosecutors, judges and lawyers, in case management and child and gender- sensitive justice. Upscale the KP model of child protection courts to address such cases. Ensure that only trained justice actors manage such cases. For many children in Pakistan, their experiences have led to feelings of shame and questioning can be a difficult and embarrassing process.

- Coordination and collaboration are key to addressing and responding to OCSEA. There are several ministries, departments and agencies that are directly or indirectly responsible for working together against OCSEA in

their respective areas of expertise.Establish a comprehensive coordination mechanism at national level for the COP to facilitate consolidated efforts and synergies for better results by involving relevant stakeholders to coordinate strategies, share information and effectively address new challenges.

- Private companies and civil society organisations can play an important role in developing technical solutions to combat OCSEA. There is a need to support the development of clear mandates and standard operating procedures for the investigation of technology-facilitated OCSEA that detail the roles and responsibilities of all agencies and stakeholders involved.

- It is recommended to integrate the theme of COP into the existing Child Protection Technical Working Groups (TWGs) to provide more holistic and effective responses to online risks and threats to children.

- The commendable efforts made by the National Task Force on Prevention and Control of Cybercrimes against Children in the past underscore the importance of reactivating and reinforcing its initiatives for continued impact and effectiveness. A new national policy with provincial action plans involving key stakeholders can serve as a long-term priority setting plan for Pakistan. It can be a valuable tool to help relevant stakeholders understand the scale of the problem and adopt coherent policies, procedures, standards, mechanisms, technologies and other responses. It can also promote cooperation and collaboration among relevant agencies, ministries, departments and provinces in all sectors.

- It is recommended that MoITT revise its "National Cyber Security Policy 2021' to address the issue of COP as part of the cyber security framework.

- It is recommended that provincial governments notify and implement child protection policies which will help to structure and organise appropriate prevention and response to OCSEA through coordination between stakeholders.

- It is important that both the government and schools ensure that the topic of COP is part of the teaching modules for computer classes and that teachers receive adequate training.

- The PTA should continue raising awareness of the importance of COP and the OCSEA among relevant private sector entities, including internet and mobile service providers, to improve understanding of the risks to children, the legal framework and internalisation of child protection policies.

Legislative Bodies: Parliament and Provincial Assemblies

- Priorities the regular review and timely updating of national and provincial laws to adapt them to the evolving technological landscape and ensure that the legal framework remains current and effective in addressing new challenges related to technological advances.
- Issue policy directives or guidelines that specify the incorporation of COP and OCSEA awareness in the national curriculum.
- Standing Committees in the National Assembly, Provincial Assemblies, and the Senate should actively monitor, review, and recommend administrative measures to enhance the implementation of PECA 2016.

US companies are required by law to report child sexual abuse material to the NCMEC or risk a fine of up to $300,000[119]. On 11 May 2022, the European Commission proposed a law to force digital companies to find, report and remove online child sexual abuse material circulating on their platforms[120]. Google, Apple and Meta's WhatsApp and Instagram could face court orders to track down photos and videos of child abuse, otherwise face hefty fines of up to 6 percent of their global turnover. The companies would also have to crack down on grooming - conversations in which abusers try to contact children inappropriately.

International Cooperation

- In order to prosecute and investigate OCSEA cases across national borders, the government must rely heavily on extraterritorial jurisdiction clauses and informal and formal channels of cooperation with law enforcement agencies. The importance of international cooperation in identifying victims and perpetrators and uncovering links between investigations in different countries is crucial. Cross-sectoral and cross-border cooperation is necessary to combat the transnational and multijurisdictional nature of crime and to ensure that perpetrators cannot take advantage of differences between national laws regarding the legality of their actions and the available penalties.

119 Bischoff, Paul. "The Rising Tide of Child Abuse Content on Social Media - Comparitech." Comparitech, 19 Feb. 2021, www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics.

120 "Commission Unveils Law to Fight Child Sexual Abuse Online Amid Swelling Privacy Fears." POLITICO, 11 May 2022, www.politico.eu/article/european-commission-propose-law-fight-child-sexual-abuse-online.

- In the context of the OCSEA, conflicts of jurisdiction may arise. The "rule of reason" is normally applied to resolve jurisdictional conflicts between states in cybercrime cases[121]. It seeks to determine which state can reasonably demonstrate the closest connection to an offence by using territoriality as the determining factor. Given the difficulties in determining where the crime was committed, and given the fact that child sexual abuse on the Internet has an enormous impact on the physical and mental well-being of the victim, it does not seem appropriate to focus only on the location of the crime, given the various needs of the victim in the criminal justice process. Therefore, it is recommended that the "rule of reason" approach in such cases should not only focus on the closest connection to the territory of a state, but must also determine which state can best serve the interests of the child victim[122].

- INTERPOL has developed specific skills and resources to combat crimes against children and provides training and promotes best practice for police in its member countries, including to help develop police skills in relation to OCSEA[123]. FIA should further strengthen cooperation with INTERPOL and use the expertise available of INTERPOL needed to meet today's challenges.

- The government should accelerate its efforts to gain access to INTERPOL's International Child Sexual Exploitation Database of images and videos to ensure effective response and proactive surveillance and avoid duplication of law enforcement efforts.

Operation Tantalio, launched by the Spanish National Police and coordinated by INTERPOL and Europol, involved authorities from 15 countries in Central and South America and Europe. The operation, which began in 2016, investigated the sharing of child sexual abuse material via mobile messaging applications and has led to 38 arrests in Latin America and Europe as of April 2017[124].

121 Witting, S. K. (2021). Transnational by Default: Online Child Sexual Abuse Respects No Borders, *The International Journal of Children›s Rights*, *29*(3), 731-764. doi: https://doi.org/10.1163/15718182-29030010

122 Ibid.

123 Capacity Building. 26 Feb. 2020, www.interpol.int/en/How-we-work/Capacity-building.

124 "Police Smash International Online Pedophile Ring." dw.com, www.dw.com/en/police-arrest-dozens-in-international-pedophile-ring-swoop/a-38474884. Accessed 16 Dec. 2022.

- There is a need to work more closely with global technology platforms and build on existing cooperation mechanisms to ensure that the digital evidence needed in OCSEA cases can be collected quickly and efficiently, including in response to data requests and content removal procedures.

- The government should seek to strengthen cooperation and strategic partnerships with international non-governmental organisations and benefit from their expertise.

Judicial Bodies

- The superior courts should develop their rules for dealing with children, which apply to all subordinate courts, to ensure the best interests of children in accordance with international human rights law and standards, and to ensure that children have prompt access to justice and remedies and have the right to participation, the right to fairness, the right to rehabilitation, the right to non-discrimination and the right to privacy.

- The judiciary should ensure that cases involving children as victims and witnesses are given high priority and processed as expeditiously as possible to avoid unnecessary delays and adjournments.

- It is recommended that arrangements be made for OCSEA cases that the testimony of child victim may be recorded via video link and the victim is not exposed to the accused or the court. If it is necessary to present a child in court, separate and safe waiting areas should be provided for child victims and witnesses without direct contact with the accused during the trial.

- Institutionalise capacity building programmes in judicial academies. These programmes should incorporate best practises and lessons learnt from the pilot projects and provide continuous training and support to justice actors to effectively and sensitively improve their skills in handling OCSEA cases.

- Institutionalisation and expansion of successful pilot models of child-sensitive justice practises by the higher judiciary, following a decision by the National Judicial Policy Making Committee in June 2019, in collaboration with civil society, through the establishment of special children's courts and training of judicial actors. These pilot models need to be further institutionalised and extended to the district level of the country.

Holding regular courses on the issue of COP is a necessary step that judicial academies in Pakistan can take to raise awareness and educate judges on the legal, social and psychological aspects of protecting children from online harm. Training programmes can cover a wide range of topics, including the legal framework for COP in Pakistan, the types of online threats children face, the impact of online abuse on children's mental health and well-being, and best practices for investigating and prosecuting cases of OCSEA. Judicial academies in Pakistan can collaborate with experts in the field of COP to design and deliver training programmes that provide judges with a comprehensive understanding of the issue.

National Human Rights Institutes (NHRIs)

- NHRIs, especially NCRC, can raise awareness about the dangers that children face online and offline and how to stay safe by collaborating with PTA and PEMRA. It is recommended that NHRIs use commonly accepted terminology in relation to OCSEA so that information and ideas can be clearly communicated.
- To enhance understanding of the purpose and provisions of the OPSC and General Comment No. 25, NHRIs should develop materials and conduct awareness programmes with key stakeholders on Pakistan's obligation and the number of actions to be taken in accordance with international treaties when cyber crimes are committed against children.
- NHRIs should thoroughly review the Lanzarote Convention, the Budapest Convention and other treaties with regard to their status in Pakistan and recommend that the Government of Pakistan take the necessary measures to combat OCSEA.
- NHRIs can monitor online platforms to ensure that they are in compliance with human rights standards and direct authorities to take remedial action and hold those responsible accountable for their actions.
- The NCRC should include the issue of COP and OCSEA in its priority area of work and examine the implementation of policy, law and child rights violations in practice.
- NCRC should develop a child-friendly complaint mechanism to facilitate easy and accessible reporting of child rights violations ensuring that children feel safe and supported when seeking help or redress.

- It is recommended that the NCRC launches mass media awareness campaigns about COP to educate parents, caregivers and children themselves about the risks of OCSEA and promote safer online practises and behaviours.

- NHRIs can conduct research to better understand the specific challenges that children face online and develop evidence-based solutions to address these challenges.

Civil Society Organisations

- Civil society organisations should further raise awareness among children, families, schools and other stakeholders about the harms and risks associated with the use of ICTs and educate them on how to protect children and the need for urgent action.

- Civil society organisations should further develop a strong advocacy and lobbying strategy to address the gap in laws enforcement for OCSEA cases, and organise training briefings for law enforcement agencies on PECA 2016.

- Further conduct quantitative and qualitative research on COP and OCSEA to understand the prevalence and impact on children, families and society and identify various bottlenecks in the implementation of existing policies, programmes and interventions and identify areas for improvement. Additionally there is a need to do research on victimology, offender profiling and new technologies.

- CSOs can strengthen partnerships with other organisations and agencies involved in COP, such as INGOs, child protection workforce, law enforcement, schools lawyers, etc. to ensure a coordinated and effective response.

- Civil society organisations may also consider translating international treaties to disseminate them to the public and key stakeholders.

- Measures should be taken to ensure ethical, informed, and balanced media coverage that respects privacy and confidentiality and puts the victim's best interests as the priority consideration.

- Media campaigns highlighting the issue and importance of COP by working with media influencers, celebrities and famous media personalities to promote the child safety agenda.

Annexure 1 Model National Response (MNR)

The Model National Response is a framework developed by WeProtect Global Alliance focused on helping countries to build their response to OCSEA.

NATIONAL COMMISSION ON
THE RIGHTS OF CHILD