JOURNAL OF LEGAL STUDIES
"Vasile Goldiș" Western University of Arad
J. L. S.
2026 – 37(51)
DOI: 10.2478/jles-2026-0005

UNMASKING ANONYMITY: THORN'S APPROACH TO COMBATING ONLINE CHILD SEXUAL EXPLOITATION IN INDIA AND ITS ADAPTABILITY TO PAKISTAN'S LEGAL FRAMEWORK

Muhammad Imran Ali*
Principal Quaid-e-Azam Law College, Kasur, Pakistan
E-mail: principal.kasur@qlc.edu.pk
ORCID: https://orcid.org/0000-0003-1395-229X

(Received: January 2026; Accepted: March 2026; Published: May 2026)

Abstract: The exponential rise of the internet has socialized the globe, and in doing so, has provided a cloak for online child sexual exploitation (OCSE). This article examines India's counter-paradigm warfare against the OECD, focusing on Thorn, a nonprofit organization using artificial intelligence, machine learning, and big data analytics to prevent and counter predator networks. India's partnership with Thorn has yielded several inspiring stories with examples of superior technologies in the investigation of culprits. However, constraints of resources and legal incongruities and lacunae remain a problem. Based on India's experience, this article analyzes the situation in Pakistan and exposes weaknesses and gaps in its cyberspace laws and enforcement. For this reason, the article calls for the adoption of Thorn's model of socio-legal analysis specifically within the socio-legal context of Pakistan. It underscores the need for allied cooperation, the question of privacy and child protection, as well as the introduction of technology into Pakistani law. Based on the objectives and findings, the article presents some practical recommendations for the Pakistani government, such as technological integration, policy modification, global networking and partnership, and capacity development. These are underscored as key measures fundamentally relevant to the establishment of a solid system of child protection, as well as guaranteeing children's protection within the digital age from acts of sexual exploitation.

Keywords: Cyber Laws; India; Online Child Sexual Exploitation (OCSE); Pakistan; Thorn.

* Corresponding author: Muhammad Imran Ali. *E-mail: principal.kasur@qlc.edu.pk*

1. Introduction

The advancement in social relations, mostly due to the impact of the internet on society, has brought about large variability in communication and business, both of which have beneficial and negative effects on societies (Antonucci, Ajrouch, & Manalel, 2017). One of the challenges is what can be described as anonymity in cyberspace, which poses a serious concern. On the one hand, it hides one's identity, thus promoting such values as freedom of speech and privacy, which are considered a major strength of democratic states (Nekrasov, Iland, Metzger, et al., 2018). But it, at the same time, provides the veil to those who exploit children sexually online by enabling them to work with impunity (Huikuri, 2023).

In India, the Prevention of Children from Sexual Offenses Act (POCSO) 2012 addresses some aspects of online child sexual exploitation (OCSE), but the law has a flaw in that offenders are shielded by a veil of anonymity. For instance, cases of encrypted messaging platforms or unknown accounts are on the rise since offenders use such channels to avoid being caught and prosecuted (Manoj et al., 2025).

To address online child sexual exploitation (OCSE), Thorn, a nonprofit organization, has adopted the use of technology such as artificial intelligence and machine learning to tackle the problem of online child sexual exploitation (OCSE) (Gurriell, 2021). This paper presents Thorn as a perfect example of how technology can help break predator networks through proactive means of handling the issue as part of the legal process that complements existing laws (Draper, 2022). For example, the use of artificial intelligence algorithms to analyze online behaviors and identify behavior patterns that indicate grooming and exploitation is a major improvement in the fight against OCSE. While it improves the practical efficiency of investigative activities, it also minimizes the perceived threat level that potential offenders face regarding identification. However, the legislation of different countries, including Pakistan, is not strong enough to address such issues.

The Pakistan Penal Code (PPC), 1860, amended by the Criminal Law (Second Amendment) Act, 2016, and the Prevention of Electronic Crime Act (PECA), 2016, collectively address online child sexual exploitation in Pakistan. These laws criminalize child pornography, cyber grooming, and sexual abuse of children. The challenge of protecting children in cyberspace is compounded by poor adoption and implementation of cyber laws. This is because online child sexual exploitation (OCSE) has no concrete laws governing its legal complexities; the nuances surrounding anonymity in cyberspace are not addressed by existing legislation (Ali, Khan & Bashir, 2022). Thus, the need for a model similar to Thorn's in Pakistan involves developing technologies and introducing reforms to current legal

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

frameworks to address such gaps. This also identifies the possible reforms, which include bringing legislation in line with current challenges, such as anonymous presence on the internet, and coordination between the police and technology companies to protect children when using the internet.

The article is a contribution to existing literature because it offers a comparative techno-legal study that links technological intervention models to legal intervention mechanisms in the fight against online child sexual exploitation (OCSE). Its added value is that it assesses the use of a technology-based investigative framework to reinforce the conventional criminal law responses in South Asia, especially in the context of the Pakistani legal system. The article is narrowed to OCSE mediated by digitally-anonymous platforms and concentrates on responses of law, institutions, and technology as opposed to victim impact measures. The article aims at achieving three goals: the analysis of the technological mechanisms applied to counteract OCSE, the evaluation of strengths and weaknesses of the Pakistani and Indian legal systems, and recommendations to provide legally effective reforms and strategies for joint enforcement measures in Pakistan. In part I of the article, the author presents anonymity, disruptive technologies, and the role of Thorn in the Indian experience. Part II analyzes the legal system and enforcement constraints of Pakistan based on a comparative understanding. Part III assesses ethical issues and offers policy suggestions to adapt the model to the Pakistani system.

2. Disruptive Technologies and Digital Justice

Disruptive technologies have fundamentally transformed digital justice systems, specifically regarding online child sexual exploitation (OCSE), a constantly evolving problem. Modern technologies, including AI, blockchain, and machine learning, have supported law enforcement agencies and judicial systems to combat OCSE with immense accuracy and speed (Ali, 2024). Advanced IT solutions orchestrated by up-to-date AI technology help to identify and classify the material rapidly and minimize the time people spend on such traumatic content as abuse. Expert systems examine large databases in search of the signs of grooming, trafficking, and exploitation and deliver operational intelligence in real time (Salem et al., 2021). In essence, this secure technology serves as a medium for preserving the chain of evidence collection and ensuring effective prosecution.

Public justice systems deploying these technologies are not devoid of some difficulties. The key challenges for further research and innovation include privacy and data protection, safety from malicious use and abuse, and addressing the problem

of algorithmic bias (Bakiner, 2023). For example, the programs that help to find victims and perpetrators and increase the general identification rates of people raise concerns about surveillance and false identification. Furthermore, the extent to which such tools are useful relies significantly on the cooperation of technology firms, international bodies, and local administration, which is not easily achievable due to systematic barriers such as jurisdictional and cultural differences.

It is not just about responding to incidents but more about proactively preventing them. The applicability of disruptive technologies comes from designing online spaces that are safer for children with filters and real-time alerts. A program like Australia's "Safety by Design" uses AI to identify risks before an individual can be hurt. In addition, through digital justice, victims gain quick, trauma-sensitive legal redress in virtual courts that are not constrained by geographical and logistical limitations (Jeffery, Atkinson & Graham, 2023).

However, it is the correlation between disruptive technologies and digital justice that indicates a potential for transformation not only in effectively eradicating OCSE but also in improving child protection. Nevertheless, continuous improvement of technological platforms, the implementation of laws that cover all aspects of technology, and more effective cooperation between states will remain crucially important for making technology an efficient tool of justice in the future.

3. Thorn for Child Safety

Thorn is fast becoming a strategic organization in the campaign against OCSE in the world through the application of modern technology and partnerships with law enforcement agencies and non-profit organizations internationally (Nikita et al., 2024). One good example in the United States is Thorn's "Spotlight' software. Thus, through elaborated machine learning algorithms implemented in Spotlight, it searches for online images related to child sexual abuse (Kjellgren, 2022). Since its creation, this tool has helped to find thousands of victims of child sexual abuse and has greatly accelerated investigations, including many arrests. The achievement of this strategy as applied in this case goes a long way in supporting the argument made regarding the use of data analytics in increasing the effectiveness of operations in this force (Lu, Lamond & Fry, 2024).

Similarly, in other countries, Thorn works with different organizations for child protection in the United Kingdom with the National Society for the Prevention of Cruelty to Children (NSPCC) (Craft, 2007). This Society has delivered educational programs for children and parents to improve their awareness of online risks. In turn, through workshops as well as producing and sharing various resources, Thorn has

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

equipped communities with knowledge and tools that can be used to prevent OCSE (Schmidt, Varese & Bucci, 2023). It has received a positive response to the initiative, proving healthy measures towards child exploitation.

The impact in Bangladesh has been significant through the local NGOs that have benefited from Thorn to protect children. Thorn has worked in offering support and education regarding the successful utilization of tools by police services to curb sexual exploitation via the internet. For example, a pilot of the introductory digital forensics and investigative training has enhanced handling of the OCSE cases and their consequential prosecution (Towhid, Nuzhat & Haque, 2023). This partnership makes it clear that while coming up with universal solutions to problems that stand in the way of improvement, such improvements must, however, be supported locally to suit the local situation, but they themselves have to adhere to international best practices.

Thus, with a range of effective strategies and proven international partnerships, Thorn has played a critical role in making the new digital context safer for children and completely proved that only the latest technology and comprehensive community involvement are the key to combating child sexual abuse.

4. Online Child Sexual Exploitation in India

Online Child Sexual Exploitation (OCSE) refers to the acts of child sexual exploitation that occur via the internet connection and bring a new issue to light in India, with multiple reports and ever-increasing trends, which make it harder to address the issue. A study done by the National Crime Records Bureau (NCRB) shows a fresh, alarming trend in the number of children sexually abused, with a good percentage of them reported to have occurred online (Daniel Manoj et al., 2025). The cases of cybercrime against children (under 18) are steadily growing from 2018 to 2022, which is an indication of the growing tendency toward online exploitation, abuse, and harassment of children (National Crime Records Bureau, 2022). Existing laws, such as the Protection of Children from Sexual Offenses (POCSO) Act, 2012, are moderately efficient in combating such heinous crimes, and, with real-time technologies and anonymous online places, the rate of enforcement becomes daunting.

The lack of, or inadequate enforcement and egalitarian application of laws, constitutes a serious impediment to the fight against OCSE in India. For example, though the POCSO has provisions for severe punishment of offenders, the enforcement structures suffer from poor training of the law-enforcing agencies in

cybercrime investigations, along with a lack of proper equipment to tackle the large networks of the internet (Juyal et al., 2017). Thirdly, the new trends like encrypted message apps like WhatsApp create almost impossible situations for tracking and arresting predators who use such apps to distribute such content (Draper, 2022). However, though the Indian government has strengthened the laws with the Information Technology (Amendment) Act, 2008, the situation is different on the ground.

There are also established cultural barriers to reporting and prosecuting OCSE cases in India to compound the problem. Lack of reporting of OCSE cases is customary due to societal pressure, while on the other hand, attitudes to victim blaming make families refrain from seeking justice (Chacko et al., 2022). The problem is the fact that most parents and their children still remain ignorant of the dangerous implications that may come out of an exchange on the internet. However, the prevention of OCSE in India will need more than just stringent laws to support the fight against it, but also awareness programs, police training, and partnerships with organizations like Thorn, which is continuously pushing for the exposure of faceless perpetrators and the defense of children in cyberspace.

5. India's Collaboration with Thorn

India's partnership with Thorn has been an effective agenda to address OCSE, especially through technological advancement and successful partnership. Thorn has leveraged newer technologies such as machine learning and artificial intelligence to assist law enforcement agencies in arresting predators. For instance, the use of the "Spotlight' operational software that analyzes child sexual abuse imagery is credited with operational efficiency (Jeglic & Winters, 2023). NCRB reports reveal that the use of such tools has helped the authorities to progress in the number of cases solved, and many children rescued and offenders brought to book under the POCSO 2012 (Tikhute, 2024).

A wonderful success story is the relationship developed between Thorn and the Cyber Crime Investigation Cell in Mumbai. As a result of this cooperation, Thorn's technology was used in active cases, in which law enforcement agencies recognized several child predators and dismantled networks that distribute CSAM (Khan, 2024). Sections 354 and 376 of the Indian Penal Code have thus received reinforcement from technological aid, which enables speedy trials against the perpetrators.

However, challenges remain; there are legal technicalities and jurisdiction barriers that make the prosecution difficult. For instance, the absence of sufficient laws on data protection and the absence of a single legal structure on cybercrime hampers the

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

gathering of evidence throughout states and hinders the progress and intricacy in conducting scrutiny. Moreover, society thrashes certain taboos that inhibit individuals who are victims of child sexual abuse from reporting the perpetrators.

Due to these obstacles, Thorn has started engaging the communities through organizational roles with the view of creating awareness and reporting options for the sociocultural issues that hinder intervention. Through having trained law enforcement and the community on OCSE prevention and implementation, Thorn has supported child safety in many ways, not only by improving investigations. This combination of legal boundaries, community participation, and technology innovation is a guide and best practice that Pakistan will find beneficial as it strengthens its own strategies against OCSE.

6. Laws Addressing Online Child Sexual Exploitation in Pakistan

Currently in Pakistan, two pieces of legislation, the Pakistan Penal Code (PPC), 1860, as amended by the Criminal Law (Second Amendment Act) 2016, and the Prevention of Electronic Crimes Act (PECA), 2016, work simultaneously to combat online child sexual exploitation. The amendments to the Pakistan Penal Code (PPC) include targeted sections, i.e., Section 292A addresses exposure to seduction, Section 292B addresses child pornography, Section 292C provides punishment for child pornography, Section 328A addresses cruelty to a child, Section 369A addresses trafficking of human beings, Section 377A addresses sexual abuse, and Section 377B provides punishment for Sexual Abuse. The Prevention of Electronic Crimes Act (PECA), 2016, addresses online child sexual exploitation through Section 20, which relates to offenses against the dignity of a natural person, Section 21, which relates to offenses against the modesty of a natural person and minor, and Section 22, which relates to child pornography.

The problem is that such laws give a general framework of how OCSE can be fought, while their applicability in addressing the intricacies of cyberspace exploitation is more of a question. PECA, especially Section 22, makes studying, preparing, publishing, and mailing child pornography a criminal offense. However, the enforcement issue has not yet been solved completely because law enforcement agencies do not have sufficient technical experience and equipment. Thus, despite the enactment of the PECA, the problem of online child sexual exploitation in Pakistan remains unaddressed because of its minor enforcement, ambiguous definitions, and lack of preparedness for technologically developing trends.

The amendments introduced into the Pakistan Penal Code by the Criminal Law (Amendment) Act 2016 put into measure the protection of children from abuse and exploitation, but are seriously lacking in the virtual world, hence failing to address the rampant issue of child predators on the internet. For instance, it contains provisions for child exploitation but lacks provisions for legal measures that address internet-based offenses, thus denying prosecution (Ali, 2023). In addition, the currently provided laws and measures do not underline the aspect of cooperation between different agencies enough in the fight against OCSE, which is highly relevant in battling the problem. Enforcement of such laws is not without some difficulties, among which is the low sensitivity of the police and the judiciary to the provisions of cybercrime laws. While dissecting their report in 2022, the Digital Rights Foundation established that many of the law enforcement agencies lack technical competency to investigate online crimes and, therefore, a low percentage of conviction rate for OCSE-related cases (Digital Rights Foundation, 2023). Moreover, due to the non-existence of a standard data protection law in Pakistan, children's data is easily exposed to any misuse (Ali, 2024). Although Pakistan has a legal framework to fight OCSE, it is a recipe for improvement, as the existing laws need a lot of reform. Pakistan can learn from India and other countries how it can serve vulnerable children better and how it can take action against those people who are involved in attacking children in the online social zone.

7. Need for Technological Intervention to Address Online Child Sexual Exploitation in Pakistan

Online Child Sexual Exploitation (OCSE) has recently become one of the most significant issues in Pakistan, mainly due to the lack of technological countermeasures as compared to India's action plans that are in vogue (Ali, 2024). In Pakistan, the laws dealing with OCSE are individual and limited. The Prevention of Electronic Crime Act (PECA), 2016, is a brief solution to deal with cybercrime. There are no specialized means for OCSE monitoring and investigations.

Nevertheless, the scarcity of specific technologies for analyzing and combating OCSE, along with the low initiative of police services, undermines activity. Notably, India has partnered with such organizations as Thorn that have helped in deploying superior technologies that include machine learning as well as big data analytics for enhanced investigations and successful prosecutions of offenders (Seto, Roche, Nicholas & Newton, 2024). For instance, the "Spotlight" tool was used by India to automatically analyze child sexual abuse imagery, and thus, women and girls are rescued faster than before from their captors. Yet Pakistan has not followed the

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

technological advancements, going through many changes in adopting new technologies, which leaves law enforcement agencies at a disadvantage regarding online crime. The Cyber Crime Wing of the Federal Investigation Agency (FIA) has, however, started making a few efforts in this regard. Yet, these efforts are quite constrained due to inadequate technical facilities and a lack of complete training among the officials (Bhatti, Adnan & Khaliq, 2021).

Furthermore, the cultural bias here in Pakistan means that people rarely report such cases. Traditional norms affect victims so that they cannot report the crime; this makes enforcement a challenge. Without adequate support in the technological environment, the existing legislation is inadequate. Therefore, replicating the best practices of India with reference to effective technologies along with policy on enhancing the legal measures in Pakistan could go a long way to enhance the fighting capability of OCSE. Such interventions would not only improve the effectiveness of investigations but also relieve the online environment for children, which is in compliance with international standards and meets the best practices in the protection of children.

8. Lessons for Pakistan from India's Insights

Online Child Sexual Exploitation (OCSE) in Pakistan can immensely benefit from importing the approaches initiated in India, wherein, considering the Thorn model, a nonprofit that has been successful in tracking child sexual abuse. Initiatives sponsored by Thorn in India have helped to build and deliver innovative digital tools like 'Spotlight' that use artificial intelligence and machine learning to help identify child sexual abuse material. Apart from speeding up investigations, these technologies have led to an increase in the rate of offenders arrested in society. The technological frameworks that are present in the definition of the new legal regulation should also be further adapted by Pakistan in order to strengthen its capacity to counteract OCSE.

This paper consolidates insights to show that by developing policies, Pakistan can encourage law enforcement agencies to make partnerships with technology companies. This cooperation could also enhance the capacity for knowledge transfer, which is of great importance in helping to build local capacity in the use of Digital and Data Forensics.

In addition, public-private partnerships may help to develop resource mobilization and innovation. For example, the use of experience gained by the e-commerce and software developers in creating similar environments to those of Thorn's systems can

be applied in a culturally appropriate manner to Pakistan's socio-structural environment. To ensure that the enforcement officials are well-prepared to use these technologies, training programs that suit international standards, particularly those familiar with Indian conditions, could be put into practice.

There is a need to make all communities involved more aware and to encourage them to report. Similar to those used in India, public awareness campaigns can include information that would help citizens to identify OCSE, know what steps to take when witnessing such an incident, and ensure that children are protected. Thus, it is possible to accomplish the goal of developing a complex approach to constructing protective domains for children in Pakistan that would cope not only with the challenges of OCSE but also create a long-term and effective model of child protection in the digital environment.

9. Collaboration with International Bodies

The propensity of online child sexual exploitation (OCSE) to be linked and spread across borders; hence, the problem cannot be combated without international efforts to deal with the crimes. International collaboration is paramount, given that OCSE often implicates networks that may be located cross-border, meaning that only one country can increasingly combat the problem. International legal instruments starting with the United Nations Convention against Transnational Organized Crime (UNTOC) include all relevant protocols that member states are expected to facilitate international cooperation in tackling crime, including OCSE. In this regard, Pakistan has ample opportunity to avail the cooperation with other formal international organizations to raise its capacity to counter OCSE.

Thorn is a good example of international cooperation with the help of cooperation with departments of different countries. Thorn is appropriating modern technologies like artificial intelligence and big data; it is also capable of effectively supporting data sharing and operations between jurisdictions. Thorn's work has seen offenders hunted and arrested across different countries, proving cooperation across borders to be effective. Currently, the United States and the Federal Bureau of Investigation FBI) cooperate through programs like the Internet Crimes Against Children (ICAC) Task Force, and as such, there is a necessity to have a cooperative approach to the investigations of transnational OCSE Cases.

In Pakistan, the cooperation with INTERPOL as well as with UNICEF can greatly strengthen the country's fight against OCSE. Pakistan needs to harmonize its laws with international norms and benchmarking to ensure easy information exchange, enforcement training, and synchronized investigation. The importance of this

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

cooperation can be stressed by the absence of technological equipment and professionals in Pakistan, which can be solved by knowledge sharing and capacity-building activities sponsored by foreign counterparts.

Also, there is the availability of a global framework, such as the Council of Europe's convention on cybercrime, also known as the Budapest Convention, that can help Pakistan to develop complete cyber laws suitable to its conditions. The establishment of such frameworks will not only help Pakistan to overturn its legal issues against OCSE, but will also best suit to authenticate Pakistan in the international domain. Therefore, international comity and cooperation, including with international organizations, remain crucially important in combating OCSE. Besides utilizing the available global programs, Pakistan should also make use of innovative sources and actively contribute to the non-recurrence and elimination of the epidemic by enhancing law enforcement performance for the protection of children from cyberspace trolling and abuse.

10. Ethical Dilemmas in Unmasking Anonymity

This is especially so in relation to freedom of information and privacy, and the rights of children against sexual exploitation and abuse online, which remains one of the most challenging human and ethical/legal questions in combating online child sexual exploitation (OCSE) (Salter, Woodlock & Wong, 2023). Privacy is one of the most cherished rights well protected by various international instruments as well as by the Constitution of Pakistan, keeping in view Article 12 of the Universal Declaration of Human Rights 1948 and Article 14 of the Constitution of Pakistan 1973. But this is not an unfettered right, especially when exercised against the background of human rights obligations like the right of children against exploitation. AI, machine learning, and big data analytics, like those deployed by Thorn, are simple to name but very effective in unmasking the anonymity of online predators. However, their use has triggered questions about invasion of privacy and also excessive spying.

In countries such as the European Union, there is a higher ground of the General Data Protection Regulation (GDPR) regarding data privacy that requires proportionality as a principle when collecting data or processing it (Hoofnagle, Sloot & Borgesius, 2019). The Indian Information Technology Act, 2000, and the amendments allow similar protections but with exceptions in the conflicting interests of national security and law enforcement agencies. Examining a number of practical cases that Thorn has implemented in India, it is clear that its tools are effective at

tracking and catching predators, but this provides an argument to create tight mechanisms to regulate the use of such technologies to avoid the opposite effect.

In Pakistan, this authority is recognized by the Prevention of Electronic Crimes Act (PECA), 2016, which partitions broad, sophisticated legal powers to the law-enforcing authorities for intercepting and monitoring electronic activities. That notwithstanding, this has raised arguments with regard to the possibility of misuse of such powers to further investigate OCSE (Yongmei & Afzal, 2023). For instance, in a number of instances, failure of the courts to review the action has resulted in the invasion of an individual's privacy with no lawful reason. A reformed surveillance system will thus need to be found in proper legislation that effectively sets the acceptable lines of conduct.

Morally, every disruption technology must meet the principles of proportionality (Bednar & Spiekermann, 2024). To protect individual rights, Thorn's model implementation in Pakistan should incorporate some measures, like the depersonalization of data and the use of judicial warrants for reporting of the intervention. An appraisal of other countries' models, for example, the United States Model "National Center for Missing & Exploited Children," shows how privacy can be accorded and still a strong protection for children can be offered. Hence, some ways can help Pakistan in eradicating these ethical dilemmas, to solve them as components of accountability and transparency of the technologies to be used, and to fulfill its duty towards the protection of children from the modality of sexual exploitation on the internet.

11. Challenges in the Implementation of Thorn's Technology in Pakistan

The implementation of Thorn to address online child sexual exploitation (OCSE) in Pakistan has several considerations, which are cultural, technical, and political in nature, that can make the program shine or fail. The first cultural concern is that society has not accepted children's sexual abuse and fails to report such cases or become actively involved in prevention. That is why cultural taboos that discourage people from speaking about cases of sexual exploitation are counterproductive in impact reduction initiatives and weaken the results of using technologies. For instance, the National Commission for the Rights of the Child (NCRC) launched a study indicating that, due to cultural barriers, many families fail to report, hence making crime statistics inadequate to support law enforcers.

On a technicality, the setup of law enforcement in Pakistan's digital frontier is not very well-developed. The country lacks resources such as trained personnel who can harness technologies such as artificial intelligence and big data analysis, which are

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

major components of Thorn's best practices. The Ministry of Information Technology and Telecommunication reveals that a majority of law enforcement organizations lack the capacity for solving cybercrimes, which supports the need for building capacity and offering training programs.

On a political level, Online Child Sexual Exploitation (OCSE) is one of the issues in Pakistan where there is no proper and effective legal framework. Though there are anti-cybersquatting laws like the Prevention of Electronic Crimes Act (PECA) 2016, they are not enforced consistently as they are affected by bureaucracies and the absence of political will. As an illustration, Section 21 of PECA, which criminalizes child porn, has significant enforcement deficiencies because of the lack of funding for prosecutors and the lack of interdepartmental coordination. In spite of such structural challenges, the Thorn model can provide a viable solution that can be implemented in Pakistan. By setting up centralized digital platforms, using AI and machine learning to detect and stop in a short period of time, and having targeted pilot programs, law enforcement agencies can be efficient even in a limited political and bureaucratic environment. Additional solutions, including public-private partnerships, international cooperation, and capacity-building efforts, will assist in getting over the bureaucracy and, at the same time, provide uniform and technology-driven protection of children on the internet.

Also, the legal framework is disintegrated, with government departments' blurring of responsibilities that slows down the executive's efforts to respond to OCSE jointly. To counter these challenges, various strategies essential for improving the protection of children in Pakistan include promoting improved perceptions of child protection, improving technical facilities, and expediting the laws for better endorsement by police departments.

Therefore, the plan of action prescribed by Thorn, thus, has the potential to work in case Pakistan targets the roots of OCSE, but realization of the entire potential of the methodologies suggested by Thorn will require tackling the cultural, technical, and political fundamentals of the South Asian nation in question. If Pakistan is willing to invest in awareness, in the infrastructure needed to protect the children, as well as in the legal reforms required to address the issue, it has everything it needs to build a better model.

12. Conclusions

On the one hand, the internet has opened numerous opportunities for children and young people. On the other hand, it has evolved into a platform for OCSE.

Addressing this challenge requires much more than technology; good laws as well as effective policies and strategies for their implementation. When utilized properly, technological advancements like those seen in unleashing the fake characters online, such as Thorn, who vigilantly exposes the characters, reveal the desirable change technology brings. Through AI, machine learning, and big data, Thorn has shown how the anonymity of predators can be eradicated so that children can safely navigate the internet. The lessons in this story of collaboration with Thorn highlight the need to mine technology more in tune with the legal and social systems, a situation Pakistan needs to fix urgently.

In Pakistan, it is the Prevention of Electronic Crimes Act (PECA), 2016. However, its efficacy in effectively addressing OCSE is the issue in question in the present study. However, there are problems, many of which require new amendments that add updated technological tools, as well as stronger filters against abuse. Policy changes should target the requirement of politicians and other official actors to reveal surveillance practices that involve the use of new technologies, which should be complemented with judicial supervision. Similarly, programs to develop the capability of enforcement agencies in using disruptive technologies for countering threats without violating people's rights to privacy and other freedoms are equally crucial.

Another important column is international cooperation. It is possible to work with Thorn and the U.S.-based National Center for Missing & Exploited Children to act as a clearinghouse for technology transfer and disseminate new information. At the same time, conditions will be fulfilled that characterize the protection of children's rights and meet international ethical standards, such as the UNCRC.

The way forward to creating a safer environment in the digital world for children is a thin line between using technology and protecting citizens' constitutional rights. Social change is achievable even if the laws are centrist, putting the rights of the children first and incorporating measures within surveillance technologies. For Pakistan, it means that by adopting a wide-ranging approach based on the use of information technology, legal framework, and international cooperation, Pakistan will fight not only OCSE but also establish global best practice in the protection of vulnerable groups in the era of cyberspace.

The major value added to this article is the fact that the technological investigational ecosystem can work as a complement to criminal justice and not an alternative to it, especially in jurisdictions facing the challenge of anonymous cyber-offending. Through the comparative analysis between India and Pakistan, the article demonstrates that this model can be applied to other developing or legally

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 81 – 97

transitional states with a weaker enforcement capability but a high level of digital penetration. However, the article is limited; it is based on doctrinal and policy review and not empirical enforcement data, and the case studies on technology might not entirely demonstrate socio-cultural obstacles to reporting or prosecution. In spite of these limitations, the results play a crucial role in the legal community by ensuring a call to judges, legislators, and investors to embrace the concepts of algorithmic evidence, cross-border partnership, and platform responsibility in the concept of safeguarding procedures. The Pakistani legal system should be developed in the future as a harmonization with international standards of child-protection and multi-stakeholder mechanisms, as India is already developing towards providing protection of constitutional rights, as well as technologically informed enforcement in cyberspace.

Acknowledgments
The author thanks the anonymous reviewers and editor for their valuable contributions.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not – for – profit sectors.

Author Contributions
The entire article was written by Muhammad Imran Ali.

Disclosure Statement
The author has no competing financial, professional, or personal interests from other parties.

References
1. Ali, A., Khan, I., & Bashir, S. (2022). Need for international legislation regarding cybercrimes: Pakistan perspective. Pakistan Journal of Social Research, 4(2), pp.136-144.
2. Ali, M. I. (2023). Need for implementation of sex education curriculum in primary schools to protect children from sexual abuse in Pakistan. Journal of Legal Studies, 31(45), pp. 51-65.
3. Ali, M. I. (2024). Unveiling the tapestry: A comparative investigation into data-protection legislation in India and Pakistan. Socrates, 1(28), pp.1-8.

4. Ali, M. I. (2024). Strategies for intervention and prevention in online child sexual exploitation. Teisė, 132, pp.145-155.
5. Antonucci, T. C., Ajrouch, K. J., & Manalel, J. A. (2017). Social relations and technology: Continuity, context, and change. Innovation in Aging, 1(3). https://doi.org/10.1093/geroni/igx029
6. Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. Big Data & Society, 10(2). https://doi.org/10.1177/20539517231205476
7. Bednar, K., & Spiekermann, S. (2024). Eliciting values for technology design with moral philosophy: An empirical exploration of effects and shortcomings. Science, Technology, & Human Values, 49(3), pp. 611-645.
8. Bhatti, S. H., Adnan, S. M., & Khaliq, A. (2021). Journal of Educational Management & Social Sciences, 2(1), pp. 79-89.
9. Chacko, A. Z., et al. (2022). A study on child sexual abuse reported by urban Indian college students. Journal of Family Medicine and Primary Care, 11(9), pp. 5072-5076.
10. Craft, A. (2007). Working together to protect children: Who should be working with whom? Archives of Disease in Childhood, 92(7), pp. 571-573.
11. Digital Rights Foundation. (2023). Digital Rights Foundation's helpline reports over 2500 cases of digital harassment in 2022. https://digitalrightsfoundation.pk/digital-rights-foundations-helpline-reports-over-2500-cases-of-digital-harassment-in-2022/
12. Draper, L. (2022). Protecting children in the age of end-to-end encryption. Joint PIJIP/TLS Research Paper Series, (80). https://digitalcommons.wcl.american.edu/research/80/
13. Gurriell, M. (2021). Born into porn but rescued by Thorn: The demand for tech companies to scan and search for child sexual abuse images. Family Court Review, 59(4).
14. Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), pp. 65–98.
15. Huikuri, S. (2023). Users of online child sexual abuse material. Journal of Police and Criminal Psychology, 38, pp. 904-913.
16. Jeffery, C. P., Atkinson, S., & Graham, C. (2023). Using the story completion method to explore Australian parent and child responses to online risk. New Media & Society, 27(4), 2212-2229.
17. Jeglic, E. L., & Winters, G. M. (2023). The role of technology in the perpetration of childhood sexual abuse: The importance of considering both in-person and online interactions. Children, 10(8), 1306.
18. Juyal, D., et al. (2017). Lack of special courts under the Protection of Children from Sexual Offences Act: A structural deficit. Journal of Family Medicine and Primary Care, 6(4), pp. 881–882.
19. Khan, A. A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. Laws MDPI, vol. 13(4), 44.

20. Kjellgren, R. (2022). Good tech, bad tech: Policing sex trafficking with big data. International Journal for Crime, Justice and Social Democracy, 11(1), pp.149-166.
21. Lu, M., Lamond, M., & Fry, D. (2024). A content analysis of metrics on online child sexual exploitation and abuse used by online content-sharing services. Child Abuse & Neglect, 157, 107046. https://doi.org/10.1016/j.chiabu.2024.107046
22. Manoj, D., et al. (2025). Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. Child Protection and Practice, 4, pp.100088.
23. National Crime Records Bureau. (2022). Crime in India. https://www.ncrb.gov.in/crime-in-india-year-wise.html?year=2022&keyword
24. Nekrasov, M., Iland, D., Metzger, M., et al. (2018). A user-driven free speech application for anonymous and verified online public group discourse. Journal of Internet Services and Applications, 9, 21.
25. Nikita, N. A., et al. (2024). Digital transformation in non-profit organizations: Strategies, challenges, and successes. Advanced International Journal of Multidisciplinary Research, 2(5), pp. 1-21.
26. Salem, H., Soria, D., & Lund, J. N., et al. (2021). A systematic review of the applications of expert systems (ES) and machine learning (ML) in clinical urology. BMC Medical Informatics and Decision Making, 21, 223.
27. Salter, M., Woodlock, D., & Wong, T. (2023). The sexual politics of technology industry responses to online child sexual exploitation during COVID-19: "This pernicious elitism." Child Abuse & Neglect. 168(2), Article 106559. https://doi.org/10.1016/j.chiabu.2023.106559
28. Schmidt, F., Varese, F., & Bucci, S. (2023). Understanding the prolonged impact of online sexual abuse occurring in childhood. Frontiers in Psychology, 14, 1281996. https://doi.org/10.3389/fpsyg.2023.1281996
29. Seto, M. C., Roche, K., Nicholas, M., & Newton, J. (2024). Predictors of online child sexual exploitation through image-sharing. Child Protection and Practice, 2. https://doi.org/10.1016/j.chipro.2024.100045
30. Tikhute, V. (2024). Children under attack: Trends and patterns of sexual offences against children in India. Journal of the College of Community Physicians of Sri Lanka, 30(10), pp. 27-36.
31. Towhid, M. I. I., Nuzhat, R., & Haque, M. A. (2023). Protecting children from online sexual abuse in Bangladesh: A policy brief. Bangabandhu Sheikh Mujib Medical University Journal, 16(2), pp. 111-117.
32. Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'The Prevention of Electronic Crimes Act, 2016' as legal support in Pakistan. Academy of Education and Social Sciences Review, 3(2), pp. 203-212.