JURNAL LITIGASI

Available online at: *journal.unpas.ac.id/index.php/litigasi*

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Online Child Sexual Exploitation and Abuse as Organized Crime: Towards a New International Legal Framework

Hesti Septianita[(1)]
Doctoral Program, Faculty of Law, Universitas Diponegoro, Semarang, Indonesia
Email: hesti.septianita@unpas.ac.id

Pujiyono[(2)]
Faculty of Law, Faculty of Law, Universitas Diponegoro, Semarang, Indonesia
Email: pujifh@yahoo.com

Irma Cahyaningtyas[(3)]
Fakultas Hukum Universitas Pasundan, Bandung, Jl. Lengkong Besar No. 68 Bandung, Jawa
Email: irmacahyaningtyas@lecturer.undip.ac.id

ABSTRACT

Online child sexual exploitation and abuse (OCSEA) has increasingly become a serious form of transnational organized crime and a grave violation of children's fundamental rights under international law. This study examines how OCSEA has evolved from localized, offline abuse into complex online operations involving darknet platforms, structured criminal networks, specialized roles, cryptocurrency-based transactions, and coordinated activity across national borders. Using a doctrinal legal method, supported by comparative jurisdictional analysis and selected law enforcement data, this research assesses whether existing international legal frameworks are adequate to address OCSEA as organized crime. The study finds that current instruments, including UN Convention against Transnational Organized Crime, the Optional Protocol to the Convention on the Rights of the Child, the Budapest Convention on Cybercrime, the Lanzarote Convention, and relevant ASEAN frameworks, still contain significant legal and institutional weaknesses. These weaknesses include inconsistent definitions, fragmented jurisdictional authority, insufficiently harmonized criminal standards, and enforcement gaps that are often exploited by organized criminal networks. The analysis further shows that OCSEA meets the core characteristics of transnational organized crime, as offenders in different jurisdictions cooperate in producing, distributing, and profiting from child sexual abuse material through advanced digital infrastructure. Based on these findings, this study argues for the development of a a binding global legal framework that standardizes criminal definitions, recognizes universal jurisdiction, strengthens cross-border cooperation, and establishes effective international monitoring mechanisms. The research contributes theoretically by reframing OCSEA within the paradigm of transnational organized crime, and normatively by proposing a more coherent direction for international legal reform.

Keywords: *Online Child Sexual Exploitation and Abuse, Child Sexual Abuse Material, Transnational Organized Crime, Darknet, International Legal Frameworks.*

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

I. INTRODUCTION

Online child sexual exploitation and abuse (OCSEA) is one of the most serious violations of children's fundamental rights in the digital era. As explained by Greijer and Doek(2025). OCSEA is an umbrella concept that covers sexually exploitative acts against children where the online environment plays a role at any stage of the offense. This includes the production, distribution, and possession of child sexual abuse material (CSAM), live-streamed abuse, online grooming, and sexual extortion. Importantly, OCSEA should not be understood as a completely separate category of crime, but rather as a technology-facilitated form of child sexual exploitation and abuse (CSEA), covering criminal conduct that involves an online or digital component.

What makes contemporary OCSEA particularly concerning is its transformation into a form of transnational organized crime. Unlike earlier patterns of child exploitation, which were often associated with isolated individual offenders, modern OCSEA increasingly involves coordinated criminal networks operating across national borders. These networks use darknet platforms, encrypted communication channels, and cryptocurrency payment systems to conceal their identities, maintain their operations, and generate profit. Their activities often reflect clear organizational structures, with members taking on specific roles in the production, distribution, and monetization of CSAM. The growing use of privacy-focused cryptocurrencies, such as Monero, has made detection even more difficult, while token-based forum systems encourage the repeated uploading and exchange of abusive material (Comolli, 2025). in 2019 alone, nearly USD 1 million in Bitcoin and Ethereum was reportedly traced to CSAM-linked wallet addresses (Chainalysis Team, 2025), showing the financial dimension of these criminal networks.

The scale of the problem is reflected in recent empirical data. The Internet Watch Foundation (IWF)(Internet Watch Foundation, 2024) reported a shap increase in CSAM-related online content, from around 57,335 URLs in 2016 to 255,598 in 2022. In 2023, the United Kingdom alone recorded 375,230 reports, representing a four percent increase from 2021 (Fleck, 2023; Septianita & Rachmie, 2024). In Canada, police-reported online sexual offences against children reached 15,630 cases between 2014 and 2022, along with 45,816 incidents involving online child pornography (Savage, 2024). In Indonesia, the Commission on Child Protection recorded 3,160 cases in 2021 (KPAI, 2021), although this number is likely far below the actual scale of the problem due to reporting and detection limitations. The COVID-19 pandemic further intensified these risks by increasing children's internet use and expanding their exposure to online spaces where exploitation may occur (Huikuri, 2023; Septianita & Rachmie, 2024). Today, children and adolescents under the age of

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

eighteen make up approximately one in three internet users worldwide (Livingstone et al., 2016; Office of Research-Innocenti, 2019), creating a larger pool of potential victims.

Despite the organized and cross-border nature of OCSEA, the existing international legal framework remains insufficient. Key legal instruments, including the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography (OPSC), the Lanzarote Convention, the Budapest Convention on Cybercrime, the United Nations Convention against Transnational Organized Crime (UNTOC), the ASEAN Convention against Trafficking in Persons (ACTIP), and ASEAN's Regional Plan of Action for the Protection of Children from Online Exploitation and Abuse, were largely developed before darknet platforms and cryptocurrency-based criminal activity became central features of OCSEA. Even the newly adopted United Nations Convention against Cybercrime does not fully address the organized and transnational dimensions of this offense. Although these instruments provide important protections, they still contain major gaps in relation to digitally facilitated crimes. These gaps include inconsistent legal definitions, fragmented jurisdictional rules, insufficiently harmonized criminal standards, and enforcement mechanism that are not fully equipped to respond to the technical sophistication of OCSEA networks. As a result, prosecutors and law enforcement agencies continue to face barriers in investigation, prosecution, coordination, and cross-border cooperation.

Existing scholarship has examined several important aspects of this issue, but there remains a significant gap in the literature. Kusumawardhani & Wulandari (2024) examined national strategies for addressing child sexual exploitation in Indonesia, while Suprapto et al. (2023) examined Indonesia's preventive measures against transnational child pornography in Southeast Asia. Dearden & Tucker (2023) studied darknet activity involving cryptocurrency and Bitcoin blockchain transactions in the context of child exploitation. Ali et al. (2023) conducted a systematic review of internet-facilitated child sexual abuse, while the Global Initiative Against Transnational Organized Crime documented organized criminal enterprises involved in OCSEA across Southeast Asia (Comolli, 2025). ECPAT (2022) also identified enforcement gaps in existing legal protections against online child sexual exploitation. These studies have contributed significantly to understanding the scope, methods, and regional dimensions of OCSEA. However, none has more comprehensively a new binding international legal instrument that expressly treats OCSEA as a form of transnational organized crime and establishes a coherent global enforcement framework.

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

II. RESEARCH METHODS

This research uses a doctrinal legal approach supported by comparative and empirical analysis. The doctrinal component examines the main international legal instruments governing OCSEA, including the OPSC, the Palermo Protocol, the Budapest Convention, the Lanzarote Convention, EU Directive 2011/93/EU, and relevant ASEAN frameworks. These instruments are assessed in terms of their scope, definitions, legal obligations, and enforcement mechanisms, particularly in light of the practical realities of contemporary OCSEA networks. The comparative component draws on case studies from several jurisdictions to understand how these instruments are interpreted and applied in practice, as well as where implementation differs across legal systems. Meanwhile, the empirical component relies on law enforcement data, investigative reports, and findings from organizations such as the Internet Watch Foundation, NCMEC, Chainalysis, EUROPOL, and the Global Initiative Against Transnational Organized Crime. These materials help ground the legal analysis in documented evidence of how OCSEA actually operates. Together, these three approaches allow the research to examine OCSEA from three connected perspectives: the law as written, the law as applied, and the criminal reality that the law seeks to address. This combined approach is necessary to identify the weaknesses in the current legal framework and to determine what a more effective international response should include.

Legally, this study conducts a systematic analysis of main international instruments, such as the United Nations Convention against Transnational Organized Crime (also known as Palermo Convention), the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography, the Budapest Convention on Cybercrime, the Lanzarote Convention among other regional and national legislations to address OCSEA, or if there genuinely remains a need for a more robust enactment. Moreover, the researcher examines how the legislation functions in social contexts; specifically, its reactions to the social issues, obstacles, and harms that accompany OCSEA.

We take a comparative approach to studying legal frameworks, with the help of comparative case studies (Salter & Mason, 2007; Simabura et al., 2023). It explores the extent to which some countries, such as the United States, Canada, the United Kingdom, Australia, Thailand, and Indonesia, recognize OCSEA networks and demonstrate features of transnational organized crime. In this comparison, the study examines how these national jurisdictions deal with such cases in practice, particularly regarding investigation, prosecution, enforcement and cross-border cooperation.

Finally, to ensure that the legal analysis in grounded in documented reality, this research draws on reports and statistical data from organizations

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

that regularly monitor OCSEA trends, including the Internet Watch Foundation, NCMEC, Chainalysis, EUROPOL, and the Global Initiative Against Transnational Organized Crime. These materials are used for two main purposes. First, they help establish the empirical scale and operational characteristics of OCSEA networks, providing a factual basis for assessing whether existing legal frameworks are adequate. Second, they are used to examine whether the obligations created by current legal instruments reflects the realities faced by law enforcement agencies in practice. For example, where a legal instrument claims to address darknet operations, cryptocurrency transactions, or cross-border coordination, this research compares those provisions with documented enforcement experience. This allow the study to assess whether the instrument is practically effective or merely aspirational. By using this approach, the conclusions regarding legal gaps are not based solely on textual interpretation, but are also supported by evidence of how the law functions, or fails to function, in real enforcement contexts.

III. RESEARCH RESULTS AND ANALYSIS

A. Conceptualizing Online Sexual Child Exploitation and Abuse as Transnational Organized Crime: From Dark Web to Boardroom

Before the internet reached a mass audience in the 1990s, child sexual abuse material (CSAM) was trafficked largely through informal networks. Prior to 1993, pictures and videos passed hand-to-hand from small sets of offenders intimately linked to personal relationships and in close geographical proximity. Trust, secrecy and face-to-face contact helped these underground networks evade detection. Consequently, geography was a limiting factor on how large of a crime could be undertaken as it necessitated some type of personal touch and there are risks to moving things in person.

That situation has changed significantly. Nowadays, one darknet platform is literally linking users on different continents, facilitating large quantities of cryptocurrency transactions and operating with a level of organization that would put some legal business structures to shame. A type of offending that was once local and network-based has evolved into a global, organized, scalable and deliberately hidden criminal system that hides from normal law enforcement channels. This is not only an infrastructural shift. It is indicative of a broader evolution in the crime: from predominantly individual offending with no real structure to transnational organized criminal groups with established roles, financial incentives and mechanisms for avoiding accountability.

Before we explore how the law is catching up to this change, a clarification of OCSEA is in order. OCSEA is all acts of sexual exploitation involving persons under the age of eighteen where either the preparation, commission or

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

conclusion of the offense has been facilitated by, involves use of, or relates to a computer system (Greijer & Doek, 2025). They are not a one crime, but an umbrella concept sweeping up a host of related behaviors—production, distribution and possession of CSAM, live-streamed abuse including live streaming trafficking in person, online grooming or child luring, sexual extortion, and the commercial exploitation through digital platforms of children (Demarco et al., 2018; Gottfried et al., 2020; Ibrahim, 2022). We Protect Global Alliance (2024) breaks the model up into three key stages CSAM operation: producing the material in photos, videos or audio; actively searching for it, viewing or attempting to view CSAM; and sharing and storing CSA. The last step is considered especially damaging, since it allows abusive content to keep circulating and to perpetuate the sexual harassment of children well beyond the time when those abuses were originally perpetrated.

The names behind that type of material have meaning in and of themselves. The label of "child pornography" is still commonly used by legislators, law enforcement officers, prosecutors and judges in many jurisdictions. Nevertheless, jurisdictions in the United States, the United Kingdom and others have more and more distanced themselves from this term because it does not express the seriousness of the harm (Criminal Division, 2023). This paper uses the term Child Sexual Abuse Materials (CSAM), aligning with its more common usage by international law enforcement agencies, because it is a better representation of the fact that such material is not content produced consensually but rather evidence of crime: a permanent record of the abuse. CSAM does not sit still once it is out there. This can be used as leverage, by coercing misuse victims to create more content, set up in-person meetings, or have their family extorted for money. It travels through networks of abusers, used to groom new victims and satisfies the urges of pedophilia collectors around the world (We Protect Global Alliance, 2024). Each illustration memorializes a specific incident of abuse against a particular child.

The production and distribution pipelines through which CSAM flows have become much more sophisticated. INHOPE (Inhope, 2022, 2024) puts these platforms associated with CSAM distribution gateways as two categories: Gateways such as social media platforms, and photo-sharing services; and Facilitators such as private servers and encrypted messaging applications. The darknet, the part of the internet not accessible via traditional search engines and which provides anonymity through decentralized peer-to-peer networks, cut across both categories. The darknet is not a single network, but rather a constellation of private darknets—some run by large organizations, some just individuals and all hosting marketplaces for drugs, arms, stolen data and CSAM (Khera, 2020). Anonymous access tools, in particular Tor—which encrypt information about users and prevent internet service providers from

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

tracking users–have made these networks accessible to a wide range of offenders (Broadhurst & Ball, 2023). The Internet Watch Foundation (IWF) discovered 931 new darknet hidden services hosting CSAM in 2021 alone, an increase of 27 percent from the prior year when 743 such sites existed (Internet Watch Foundation, 2021). Other studies suggest that OCSEA-related content accounts for approximately 2 percent of Tor hidden services yet also claim that over three-quarters are directed toward OCSEA websites–which reflects a discrepancy between demand and supply where demand exists for much greater quantities of this material than there is infrastructure to hose these sites (Finklea, 2017; Owen & Savage, 2015).

Cryptocurrency has become a major financial mechanism within this ecosystem. Privacy-focused cryptocurrencies, such as Monero, allow offenders to carry out transactions with a high degree of anonymity. At the same time, token-based forum economies reward users who upload new material, effectively turning the production and circulation of abuse content into a gamified system (Comolli, 2025). In 2019, nearly USD 1 million in Bitcoin and Ethereum was traced to wallet addresses linked to CSAM (Chainalysis Team, 2020, 2025). More recently, Chainalysis identified one of the largest active CSAM darknet sites as having received more than USD 530,000 in cryptocurrency payments through over 5,800 addresses since July 2022. This exceeded the scale of the well-known 2017 "Welcome to Video" case (Chainalysis Team, 2025).

Artificial intelligence has added another layer of complexity to this already serious problem. AI-optimized models are now being used to generate highly realistic images depicting children even where no direct contact offense has occurred (Rainn, 2025). In response, the United Kingdom has introduced the Crime and Policing Bill 2025, which creates new criminal offenses targeting the production and distribution of AI-generated CSAM (Ministry of Justice. Home Office, 2025)

The empirical scale of OCSEA highlights both the urgency of the problem and the difficulty or regulating it effectively. In 2024, the IWF assessed 424,047 reports in the United Kingdom alone, representing an 8 percent increase from 2023. Of the reports, 291, 273 were confirmed to contain CSAM, while 729, 696 items were assessed as criminal material (Internet Watch Foundation, 2024). Globally, the National Centre for Missing and Exploited Children's 2024 report recorded approximately 36 million reports of suspected CSAM submitted to its international tipline (National Centre of Missing or Exploited Children (NCMEC), 2024) In Indonesia, the Commission on Child Protection (KPAI) recorded 2,057 cases of child abuse in 2024, with child pornography and cybercrime accounting for approximately 2 percent of reported cases. This figure is likely to be a significant underestimate, given the limitations of

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

detection and reporting in the region (Humas KPAI, 2024). Even these figures do not capture the full scope of the problem, as the darknet is specifically designed to conceal the true scale of activity occurring within it.

Taken together, the scope of OCSEA, the sophistication of the networks involved, the role of enabling technologies, and the scale of documented harm all point to the same conclusion: this is no longer a crime that can be understood or addressed through frameworks designed for isolated offenders or pre-digital forms of exploitation. The central question, therefore, is whether the current international legal architecture has kept pace with this reality, or whether it remains structurally tied to a world that no longer exists.

B. Online Child Sexual Exploitation and Abuse (OCSEA) as Transnational Organized Crime: Conceptual Tensions and Analytical Framework

Steeped stereotypes which confuse more than explain, discussions of cybercrime and organized crime are invariably a tale of two cities. The solitary hacker working alone in a dark room is an image which completely misrepresents the collaborative and connected nature of much cybercrime. Historical definitions of organized crime have frequently struggled to catch up with the phenomenon as it evolves. Interestingly, the line between "cyber-native" criminal groups versus traditional terrestrial crime organizations that have embraced digital tools is increasingly blurred (Broadhurst et al., 2014; Gannon et al., 2023). Thus, to understand where OCSEA fits into this landscape is to go beyond stereotypes and seek out evidenced views with care.

Organized child sexual exploitation is not a new phenomenon. Belanger et al. as early as 1984, discovered multinational organized child exploitation services that laundered both CSAM and finances to lessen the chance of detection by law enforcement. This structure anticipated key aspects of how darknet CSAM networks function today (Huikuri, 2023). What has changed, however is the scale of the activity, the technological infrastructure that supports it, and the degree of organizational sophistication involved. OCSEA now encompasses three broad operational stages: the production, distribution, and downloading of abusive material (Comolli, 2025). Each stage may involve different participants performing specialized functions. Commercial CSAM, where users pay for access to or the ability to download abusive material, has become one of the fastest-growing forms of internet crime. According to the Global Initiative Against Transnational Organized Crime, it generates an estimated annual revenue of three billion dollars globally (Septianita & Rachmie, 2024)

These characteristics have led law enforcement agencies, media organizations, and scholars to describe darknet CSAM forums as organized criminal operations (EUROPOL, 2025; Jenkins, 2001). Investigative agencies

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

have also increasingly considered whether OCSEA can be prosecuted within organized crime frameworks and whether perpetrators qualify for organized crime charges.

Yet classifying OCSEA as organized crime purely in terms of the outrage it provokes, or on emotional concerns more generally, causes conceptual confusion between academic understanding and policy application (Lavorgna & Sergi, 2016; Leukfeldt et al., 2017; Lusthaus, 2013). A more scrupulous approach would entail questioning whether or not OCSEA networks substantively satisfy the constitutive elements of organized crime, and clarifying which specific conditions they meet in doing so.

There is an undeniable and unresolved tension in the academic literature on this question. The evidence for structural complexity is strong on one side. OCSEA rings are often transnational in nature, involving organized hierarchies with designated roles for recruiting, facilitating, and receiving payment (Brodowski, 2016; Comolli, 2025; UNODC, 2014). According to Comolli (2025), OCSEA can be dealt with an organized crime approach, drawing from a wider range of law enforcement and private sector actors such as technology companies and financial institutions when there are networks, and financial gain is a primary motive. One clear example of this reality is Operation Endeavour which involved an operational investigation from 2012 to 2014 by law enforcement officials from the United Kingdom, the United States, and Australia. Investigators have identified an organized crime group based in the Philippines who live-streamed children being sexually abused to paying foreign customers in 14 jurisdictions across the globe, including the United States, Hong Kong, Taiwan, Australia and many countries in Europe (BBC, 2014; US Immigration and Customs Enforcement, 2014). The cross-border monetary transactions, the division of labor between facilitators in the victim's country and customers abroad, as well as commercial orientation of the operation, show recognizable signs of organized crime.

Conversely, van der Bruggen & Blokland (2021) provide evidence that adds unambiguous complication to any kind of black-and-white definition. Their research characterized the associational and entrepreneurial structure of darknet CSAM forums that serve to fulfill both social and criminal needs of its members. In fact, the modality of these forums often works off a trust-based hierarchy with various forms of internal governance by key actors. Yet many of these forums are essentially devoid of most aspects central to classical definitions of organized crime, such as monetary gain, physical violence and the urge to monopolize criminal markets. This discovery embedded upon Von Lampe's tripartite structure of governance: entrepreneur, associational and illegal as various types that may inform organized criminal conduct (von Lampe, 2016, 2026). Using this framework, they find that there are quite

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

significant levels of entrepreneurial and social organization in CSAM offending via the darknet—regardless of its stark divergence from classic models of organized crime (e.g. say compared to drug trafficking cartels).

Even though such a stark contrast between evidence of some level of structural organization and relative absence of traditional organized crime indicators provide tension, it does not diminish the argument that OCSEA should be treated as a form of organized crime. Rather, it refines the argument. The analytical task is not determining whether OCSEA belongs to a static and uniform category of organized crime, but for which exact arrangements it does. This paper contends that OCSEA is transnational organized crime if all of the following three elements are present: identifiable organizational structures with defined roles and internal governance mechanisms; organizational coordination among participants in multiple jurisdictions; and a profit motive, either financial or material to support the network. However, not every OCSEA offender or network will check the three conditions simultaneously. Individual offenders whose actions are primarily motivated by gratification and who operate as lone actors fall into one category, while another distinct category consists of coordinated transnational enterprises producing and distributing CSAM at a scale for commercial purposes. However, the key and troubling point is that a substantial part, and increasingly so, of contemporary OCSEA activity does satisfy these conditions. It is self-evidently this segment that existing international legal regimes are least able to govern.

This characterization is supported by a number of key features of modern OCSEA networks. Darknet forums are not simply content reservoirs, rather they compose a comprehensive operational ecosystem. These process not only the physical network, but also enable further abusive material distribution, allow exploitative behavior to be normalized, pass long knowledge of grooming techniques and evading law enforcement as well as offer financial infrastructure, with even internal escrow service specifically structured to protect members from transactional fraud (Holt et al., 2015; Hout & Bingham, 2013; Lusthaus, 2013; van der Bruggen & Blokland, 2021). Forum administrators and moderators also engage in a kind of partial market governance through, for example, the banning of users engaged in fraudulent behavior. These practices develop internal accountability structures that are, in practical terms, less dissimilar to the governing mechanisms present in traditional criminal organizations (Ministry of Justice. Home Office, 2025). New entrants usually must meet the criteria, including the publication of original CSAM, before attaining full membership status. From there, they can work their way up through pyramid levels that incentivize more extensive involvement (Gannon et al., 2023; Motoyama et al., 2011). CSAM has even been used as a gatekeeping mechanism by some actors who are motivated to share CSAM for fanbase

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

sexual purposes in a few documented instances. Those looking to join drug cartels and ideologically driven groups, for instance, have been said to order potential recruits to download CSAM on their devices as a test of loyalty. This highlights a wider coming together between OCSEA and other avenues of organized criminality (Comolli, 2025).

The geographical dimension of these networks only reinforces the potential classification of OCSEA as transnational organized crime. Local and community-level rings, some closely tied to trafficking networks, locally recruit children, produce CSAM and conduct live-streamed abuse on-demand for paying foreign customers (ECPAT, 2022). Since demand usually originates abroad, particularly in the case of affluent networks of perpetrators that exists across Western countries and other areas, highbrow buyers pay for access to these large-scale CSAM collections. Facilitators usually stay in the country of the victim, while customers and money moves across borders. It establishes a transnational division of labor that closely mirrors the functional organization of other acknowledged varieties of transnational organized crime (BBC, 2014). Research by the United Kingdom's National Assessment Centre confirms this pattern, expressing high confidence that OCSEA predominantly operates through collaborative offender networks rather than isolated individual activity. In 2025, 63 UK-based users of a darknet CSAM site were identified alongside 1,275 users worldwide. These users had either paid for access using cryptocurrency or earned access by uploading their own material, receiving site-specific credits that could be redeemed for further content (National Crime Agency, 2025).

Collectively, this evidence lends qualified support to a decisive conclusion: modern OCSEA, in its networked, cross-border, and profit-oriented configurations, satisfies the constitutive criteria of transnational organized crime. While old age indicators, particularly physical violence and marketplace monopolization—abound absent, these data centers evidence are less a marker of the cybercriminal environment than a reflection of the nature of darknet hospitality itself. The removal of physical geography, combined with anonymity tools, reduces the role of violence as a competitive or protective mechanism and makes monopolistic control over criminal markets more difficult to sustain ((Comolli, 2025; Lusthaus, 2013). These features are adaptations to a specific operating environment, not evidence that organizational structure is absent. This shift toward more sophisticated, networked, and organized forms of exploitation therefore demands a corresponding analytical and legal response. Such a response must move beyond frameworks designed primarily for individual offenders and engage seriously with OCSEA as the form of transnational organized crime that, in its most harmful manifestations, it has become.

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

C. Analyzing Current International Legal Responses to OCSEA

1. Current Legal Frameworks and Instruments

Global legal responses to OCSEA operate through an interconnected system of international and regional instruments, each addressing different dimensions of the problem. The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography (OPSC, 2000) serves as the foundational child-specific treaty in this area. It requires states to criminalize the production, distribution, and possession of child sexual abuse material, while establishing obligations relating to international cooperation and victim assistance. However, they OPSC is increasingly regarded as insufficient for addressing the contemporary scale and complexity of OCSEA. Adopted during the early phase of internet development, it does not fully account for the evidentiary and jurisdictional challenges posed by today's online offending, particularly where evidence, offenders, victims, platforms, and financial flows span multiple countries and continents.

The growing number of OCSEA victims demonstrates that this form of abuse can no longer be treated as routine or addressed only through conventional legal response (Mardin et al., 2022). To address the technological dimension of the problem, the Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention (2001), provides the most comprehensive international framework for computer-facilitated offenses. It includes specific provisions criminalizing child pornography produced through computer systems under Article 9, while also establishing procedures for cross-border electronic evidence collection, real-time traffic data interception, and the expedited preservation of stored computer data. The Lanzarote Convention (2007) further strengthens the child protection framework by expanding criminalization beyond traditional forms of exploitation. It covers online grooming, solicitation through information and communication technologies, and knowing access to child sexual abuse material even without downloading. It also establishes prevention obligations and victim support requirements, making it one of the most comprehensive legal instruments for addressing child sexual exploitation and abuse in both offline and online settings.

Together, the UN Convention on the Rights of the Child (UNCRC), OPSC, Lanzarote Convention, and Directive 2011/93/EU, provides an important legislative framework for addressing OCSEA. These instruments adopt a victim-centered approach grounded in the best interests of the child. They seek to ensure robust protection mechanisms, access to justice and remedies for child victims, specialized support services, psychological

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

counseling, and social reintegration. They also emphasize prevention through education and awareness-raising, require multidisciplinary cooperation among law enforcement, child protection services, and judicial authorities, and oblige states to criminalize all forms of child sexual exploitation and abuse with appropriate sanctions. At the same time, they require that children's dignity, privacy, and rights be safeguarded throughout investigation and prosecution processes.

The most recent instrument, the UN Convention against Cybercrime (the Hanoi Convention) was adopted in 2024 and represents the first global treaty that criminalizes online child sexual exploitation and abuse, child abuse materials, and related forms of technology-facilitated offending. It requires states to adopt measures to protect children from the misuse of technology by online predators. It also encourages cooperation among a wide range of institutional partners and stakeholders, while emphasizing that children should be placed at the center of these joint efforts and that their views should be heard and respected (Novianti & Chusairi, 2024; Voziki, 2021).

The Lanzarote Convention (2007) provides broad and detailed coverage of child sexual exploitation and abuse, including online grooming and ICT-facilitated solicitation. However, its regional character limits its global application. By contrast, the UN Convention against Transnational Organized Crime (UNTOC, 2000) provides a global framework for addressing transnational organized criminal groups and networks, but it does not explicitly address organized OCSEA networks.

The UN Convention against Cybercrime, opened for signature in October 2025, criminalizes a wide range of conduct related to child sexual abuse and exploitation material. This includes producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing, or otherwise making such material available through an information and communications technology system. It also covers soliciting, procuring, accessing, processing, or controlling child sexual abuse or exploitation material stored in an ICT system or another storage medium, as well as financing these offenses. This new legal framework has raised hopes for a stronger global response to crimes committed against children. However, its effectiveness remains limited by participation. Only 74 countries have signed the treaty, while several countries with high numbers of OCSEA cases and significant circulation of CSAM, including the United States of America and Indonesia, are not yet state parties.

Despites the adoption of these legal instruments, there remains no specific legal framework that addresses OCSEA as a form of transnational organized crime. This gap is significant because OCSEA is often committed

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

by organized groups of offenders, regardless of whether the individuals involved know one another personally. The modus operandi of many OCSEA networks reflects the definition of an organized criminal group under the Palermo Convention on Transnational Organized Crime. Given the grave violations against children's rights involved, it is crucial to recognize this particular form of offending as transnational organized crime. For this reason, Santoso & Musyayyadah (2025) argue that existing legal norms must be reinterpreted and reoriented to ensure that children's rights are effectively protected.

2. Addressing OCSEA as Transnational Organized Crime and Systematic Gap Among International Legal Frameworks

This research seeks to identify systematic gaps in existing international legal frameworks and to argue for the development of new, specific legal instruments capable of addressing transnational organized OCSEA more effectively.

The legal frameworks examined in this analysis include the UN Convention against Transnational Organized Crime (UNTOC, 2000) and its Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children; the UN Convention against Cybercrime (2024); the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, Child Pornography; The Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention; the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; Directive 2011/93/EU of the European Parliament and of the Council on 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography; and the ASEAN Convention against Trafficking in Persons, Especially Women and Children (ACTIP).

Taken together, these international and regional instruments address important aspects of transnational crime, cybercrime, trafficking, and child protection. However, they also reveal significant systematic gaps in coordination, scope, and enforcement. These gaps make it difficult to respond comprehensively to evolving forms of harm such as online child sexual exploitation and abuse.

A fundamental problem lies in the jurisdictional and definitional inconsistencies across these frameworks. The Trafficking Protocol supplementing UNTOC focuses primarily on trafficking for the purpose of exploitation, but it does not adequately address non-commercial sexual abuse or the digital dimension of exploitation.

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography establishes important minimum standards for criminalizing these offenses and emphasizes state obligation. However, its definitions may diverge from those used in regional instruments, and it lacks detailed provisions for the rapidly evolving digital environment in which most CSAM is now produced, exchanged, and distributed.

The Budapest Convention on Cybercrime was groundbreaking in addressing computer-related crimes and includes provisions on CSAM. Nevertheless, it treats CSAM as one category among many cybercrime offenses and does not provide the comprehensive victim-centered approach found in child protection instruments such as the Lanzarote Convention.

The Lanzarote Convention offers one of the strongest framework for preventing and combating the sexual exploitation and sexual abuse of children, including online grooming and solicitation. Its major limitation, however, is in its geographic reach. Because it is primarily a Council of Europe instrument, its global applicability remains limited, even though OCSEA frequently involves offenders, victims, platforms, and financial flows spread across multiple regions.

Similarly, Directive 2011/93/EU establishes strong regional standards for harmonizing offenses, strengthening victim protection, and improving prosecution within the Europe Union. Yet enforcement gaps arise when crimes involve offenders, victims, or service providers located outside EU jurisdiction.

The ASEAN framework operates through several layers. ACTIP demonstrates regional commitment to combating trafficking in persons, especially women and children, but it contains weak enforcement mechanisms and limited provisions on cyber-enabled exploitation. The ASEAN Regional Plan of Action on the Elimination of Violence Against Children provides a broader strategic framework, but remains largely aspirational. More recently, the Regional Plan for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN represents a more targeted attempt to address digital threats. However, these ASEAN instruments are largely non-binding action plans rather that enforceable legal strategies. They also lack dedicated implementation and monitoring mechanisms with meaningful accountability. In addition, ASEAN's traditional emphasis on non-interference in the domestic affairs of member states continues to constrain coordinated cross-border responses.

The newly adopted UN Convention Against Cybercrime attempts to bridge some of these gaps by creating a broader global framework for cybercrime cooperation. However, it has also faced criticism for potentially

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

weak human rights safeguards and for treating OCSEA as part of a broader cybercrime agenda rather than as a distinct and urgent form of translational organized exploitation. As a result, despite the existence of multiple international and regional instruments, no current framework fully addresses OCSEA as a specific form of transnational organized crime.

3. Gaps in the Current International Legal Framework and the Case for Reform

The instruments assessed in this research, including the OPSC, the Palermo Protocol, the Budapest Convention, the Lanzarote Convention, EU Directive 2011/93/EU, the UN Convention against Cybercrime, and various ASEAN frameworks, were developed independently for various purposes and at different points in time. As a result, they do not form a coherent system. Some areas overlap, some are gaps, and the use language used is inconsistent across the board. These are not just technical issues. These are structural vulnerabilities that organized criminal networks have honed in on and take advantage of.

We identify six key gaps, which are interconnected and common across the international legal environment.

The first gap is definitional inconsistency. Different instruments use different terms to describe the same or closely related conduct. The OPSC, for example, still uses the term "child pornography," while the Lanzarote Convention and EU Directive refer to "child sexual abuse material." This is not simply a matter of wording. Different definitions reflect different understandings of the crime, and these differences create practical obstacles when states attempt to cooperate on prosecutions, extradition, and mutual legal assistance requests. The problem is also visible at the regional level, where ASEAN member states continue to show wide variation in domestic legislation despite repeated regional calls for harmonization.

The second gap is the absence of a framework in which OCSEA can be understood as the complex, interrelated criminal phenomenon it often is. In real life, sex trafficking and cybercrime are often closely related. Children are groomed, abused to capture material and sometimes trafficked in a single operation. No one want to measure the entire continuum. Fragmentation within ASEAN across ACTIP, the other regional plan on ending violence against children and the only dedicated regional framework on online exploitation poses coordination challenges, deepened uncertainties about responsibilities. These weaknesses, as Morales & Castillo (2025) argue, can serve to perpetuate systemic impunity and the institutional inertia that enables them directly determine not only measure

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

the depth of their impact on victims but also cover up ever ends up hindering meaningful progress.

Third, there is a large gulf of difference between instruments that create legally binding obligations and those that are truly non-binding in nature. Conventions such as the Palermo Protocol, the Budapest Convention, and the Lanzarote Convention create concrete legal duties for states. ASEAN's regional actions plans are lacking in this regard. Devoid of punishment for non-compliance, they depend on voluntary adherence. The ASEAN Regional Plan of Action on online exploitation identifies the relevant problems clearly and proposes reasonable responses. However, without legal force, resources dedicated to their implementation, critical timelines for implementation, or monitoring mechanisms for compliance, there is little assurance that these pledges will become part of national law and practice.

Fourth, enforcement capacity is still profoundly disparate. A lot of countries do not have the technical facilities, funding or even political will for them to enact these conventions. The current architecture of existing human rights monitoring bodies to enforce international children and youth-related treaties mostly works in silos without systematic information-exchange or coordinated follow-up. In the ASEAN context, this problem is worsened by the region's culture of consensus-based decision-making and strong norm of non-interference. As a result, no global entity can enforce adherence, resulting in states with lax legislation or ineffective enforcement becoming havens for offenders.

Fifth, most of these instruments were not designed to address the realities of contemporary OCSEA. Live-streamed abuse, encrypted communications, weak or inadequate age-verification system on digital platforms, and AI-generated abuse material were not the kinds of challenges that the drafters of the OPSC in 2000 or the Budapest Convention in 2001 were confronting. ASEAN's more recent regional plan on online exploitation does acknowledge these developments, but recognizing a problem is not the same as having the operational capacity to address it. Across many member states, the gap between acknowledgement and implementation remains substantial. The same can be said of the UN Convention on Cybercrime. Like the ASEAN frameworks, it attempts to adapt to emerging technologies. However, adaptation does not necessarily amount to adequacy. As long as OCSEA is treated as primarily a cybercrime rather than a form of transnational organized crime, the full range of organized crime law enforcement tools, including asset forfeiture, enterprise liability, and coordinated network dismantlement, remains largely unavailable or underused.

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Sixth, the geographic fragmentation of these frameworks creates jurisdictional spaces that offenders can deliberately exploit. ASEAN instruments lack the binding force of their European counterparts, while global and European frameworks often face implementation challenges in Southeast Asia because of differences in legal traditions, resources, enforcement capacity, and political priorities. A single offender may groom a child in one country, commission the production of abuse material in a second, store the material on servers in a third, and distribute it through platforms registered in a fourth. In doing so, offenders can target jurisdictions with weaker laws, limited enforcement capacity, or slow mutual legal assistance procedures. The current system does not merely allow this kind of fragmentation; in practice, it often makes it relatively easy to exploit.

Before making the case for a new framework, it is important to be clear about where this research stands in relation to what has already been done, and where the existing scholarship and legal instruments still fall short.

In relation to OCSEA, much of the existing scholarship approaches the problem through one of several tried and tested lenses. A few studies examine child protection and victim welfare (Livingstone et al., 2016; We Protect Global Alliance, 2024). Some approach OCSEA primarily as cybercrime problem, focusing especially on platform governance, digital forensics or technical aspects of darknet activity (Broadhurst & Ball, 2023; Dearden & Tucker, 2023). The third strand rather views OCSEA in the context of trafficking and sexual exploitation (particularly in terms of modelling recruitment and regional dynamic patterns) (ECPAT, 2022; Suprapto et al., 2023). They moved closer to an organized crime framing by documenting the structural features of OCSEA networks in Southeast Asia (Comolli, 2025; Global Initiative Against Transnational Organized Crime, 2014). These studies, however, also do not systematically assess the adequacy of existing international legal instruments to address OCSEA as a modern form of transnational organized crime. They also do not make any suggestion to create a new binding international legal framework for the purpose.

This research occupies that gap. It does not treat OCSEA simply as a child welfare issue, a cybercrime issue or a trafficking issue, though it is all of these things. Instead, it views OCSEA as a new kind of transnational organized crime and then asks the question whether or not international frameworks are properly suited to address that type of crime. The answer this research reaches is that they are not. This is not because the individual instruments are poorly designed, but because they were created for different purposes, at different times, and without the coordinating

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

architecture needed to address a crime that operates across all of them simultaneously.

This research, therefore, proposes something more than patchwork amendments to existing instruments. That is why it is also an argument for a bespoke, binding international legal framework founded from first principles on OCSEA as organized crime.

4. The Case for a Unified Global Framework

The Internet Watch Foundation documents millions of CSAM URLs every year. Live-streamed abuse continues to expand, particularly across Southeast Asia. At the same time, AI-generated abuse material and encrypted platforms are creating new avenues for exploitation that existing legal frameworks were never designed to address. Law enforcement agencies are therefore left to navigate incompatible legal definitions, slow cross-border procedures, mismatched investigative powers, and major disparities in technical capacity between wealthier and less-resourced countries.

A unified global framework would need to go significantly beyond what current instruments provide. It would require the mandatory criminalization of all forms of OCSEA, including grooming, solicitation, possession, distribution, and production, based on consistent definitions and proportionate penalties across jurisdictions. It would also require extraterritorial jurisdiction, so that offenders cannot avoid prosecution simply by crossing borders. In addition, such a framework would need faster and more streamlined evidence-sharing mechanisms capable of keeping pace with digital crime; clear and enforceable obligations for technology companies and internet service providers to detect, report, and remove abuse material; guaranteed support and remedies for child survivors regardless of where they live; dedicated funding for capacity-building in countries where OCSEA is most prevalent and resources are most limited; and a credible international monitoring body with real authority to coordinate investigations, facilitate information exchange, and hold states accountable when they fail to meet their obligations.

The transnational character of OCSEA also requires international cooperation that extends beyond prosecution. Cooperation must include the identification, protection and recovery of victims. Accordingly, international cooperation should not be oriented solely toward strengthening law enforcement against offenders, but must also include victim-sensitive mechanisms to ensure that child victims of OCSEA are accurately identified before any criminal liability is imposed on them (Maharani et al., 2026).

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Without such a framework, children's safety will continue to depend largely on the accident of where they happen to live. Offenders will continue to exploit legal inconsistencies. Investigations will continue to collapse under bureaucratic obstacles. And the children most at risk, particularly those in countries with weak governance and overstretched resources, will continue to bear a disproportionate share of the harm.

Protecting children from sexual exploitation in digital spaces is a basic human rights obligation. Children are not only rights-holders in the present, but also vital members of society whose protection is essential to a country's future (Nuridah et al., 2025). The current fragmented and reactive approach is no longer adequate. The evidence examined in this research makes a clear case for replacing it with a framework that is proactive, unified, enforceable, and centered on the protection of child victims.

Accordingly, any inter-state cooperation must include victim-sensitive mechanisms to prevent child victims of OCSEA from facing criminal responsibility or other negative legal consequences before they are correctly identified.

IV. CONCLUSIONS

Existing international legal frameworks were not prepared to account for the structural transformation of online child sexual exploitation and abuse (OCSEA). What was once perhaps seen only in insolated individual instances of offending has over time, in its most organized forms, become a transnational criminal enterprise. They run transnational networks, taking advantage of technological infrastructure and within this context considerable sums of money. OCSEA does not always meet the threshold for transnational organized crime. We argue that OCSEA does not fulfill these criteria unless three conditions are satisfied: identifiable organizational structures, operations spanning multiple jurisdictions, and the pursuit of profit by the network. This segment of OCSEA represents the greatest challenge of enforcement and is least sufficiently addressed by existing international legal regimes.

The findings considered in this analysis suggest an exclusive, mandatory international legal regime established from scratch. That framework should harmonize definitions of crime, assert extraterritorial jurisdiction, simplify cross-border evidence sharing, impose clear responsibilities on technology platforms, provide remedies and support for survivors, deliver resources to the least resourced countries and set up a truly powerful international monitoring body.

Lacking a coordinated and enforceable response of this kind, OCSEA networks will continue to exploit the fragmentation of legal protection, jurisdictional gaps and disparities in enforcement capacities. Hence, a common

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

global frame is not just a legal reform idea. This is an important step in the fight against one of the most grievous and emergent threats to children and represents a form of transnational organized crime.

BIBILIOGRAPHY

Alejandro Morales, S., & Castillo, A. (2025). *The Case of Gender Violence in Mexico: Does the Judicial System Ensure Substantive Justice for Victims? ¿Garantiza el Sistema Judicial la Justicia Sustantiva para las Víctimas?* (Vol. 1). https://publications.socipol.org/index.php/cjs/index

Ali, S., Haykal, H. A., & Youssef, E. Y. M. (2023). Child Sexual Abuse and the Internet—A Systematic Review. *Human Arenas*, *6*(2), 404–421. https://doi.org/10.1007/s42087-021-00228-9

BBC, U. (2014, January 16). *Philippines web abuse ring smashed in UK-led\operation*. BBC UK. https://www.bbc.co.uk/news/uk-25749326.

Broadhurst, R., & Ball, M. (2023). How the World'S Biggest Dark Web Platform Spreads Millions of Items of Child Sex Abuse Material — and Why It's Hard to Stop. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4364472

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. In *International Journal of Cyber Criminology* (Vol. 8, Number 1). http://www.verizonenterprise.com/resources/reports/rp_data-

Brodowski, D. (2016). *International Law and Transnational Organized Crime* (P. Hauck & S. Peterke, Eds.). OxfordAcademic. https://doi.org/https://doi.org/10.1093/law/9780198733737.003.0016

Chainalysis Team. (2020). *Making Cryptocurrency Part of the Solution to Human Trafficking*. Chainalysis. https://www.chainalysis.com/blog/cryptocurrency-human-trafficking-2020/.

Chainalysis Team. (2025, July 28). *Chainalysis Identifies Large CSAM Website Using Cryptocurrency*. Chainalysis. https://www.chainalysis.com/blog/chainalysis-identifies-large-csam-website-using-cryptocurrency-july-2025/

Comolli, V. (2025). *Organized Child Sexual Exploitation. Addressing Motives and Response Need in South East Asia.* https://globalinitiative.net/analysis/organized-child-sexual-exploitation/.

Criminal Division. (2023, August 11). *Child Pornography*. US Dept of Justice. https://www.justice.gov/criminal/criminal-ceos/child-pornography.

Dearden, T. E., & Tucker, S. E. (2023). Follow the Money: Analyzing Darknet Activity Using Cryptocurrency and the Bitcoin Blockchain. *Journal of Contemporary Criminal Justice*, *39*(2), 257–275. https://doi.org/10.1177/10439862231157521

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Demarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation A Rapid Evidence Assessment Final Report*. www.iicsa.org.uk.

ECPAT, I. and UNICEF. (2022). *Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse, Global Partnership to End Violence Against Children*. https://www.unicef.org/philippines/media/7396/file/Disrupting%20Harm%20in%20the%20Philippines.pdf

EUROPOL. (2025). *Child Sexual Exploitation*. EUROPOL. https://www.europol.europa.eu/crime-areas/child-sexual-exploitation.

Finklea, K. (2017). *Dark Web Kristin Finklea Specialist in Domestic Security*. www.crs.gov

Fleck, A. (2023). *Online Child Pornography Skyrockets*. Statista.Com. statista.com/chart/30964/

Gannon, C., Blokland, A. A. J., Huikuri, S., Babchishin, K. M., & Lehmann, R. J. B. (2023). Child sexual abuse material on the darknet. *Forensische Psychiatrie, Psychologie, Kriminologie*, *17*(4), 353–365. https://doi.org/10.1007/s11757-023-00790-8

Global Initiative Against Transnational Organized Crime. (2014). *Stollen innocence,The Online Sexual Exploitation of Children*. GlobalInitiativeAgainstTransnationalOrganizedCrime. https://globalinitiative.net/analysis/stolen-innocence-the-online-exploitation-of-children/

Gottfried, E. D., Shier, E. K., & Mulay, A. L. (2020). Child Pornography and Online Sexual Solicitation. *Current Psychiatry Reports*, *22*(3), 10. https://doi.org/10.1007/s11920-020-1132-y

Greijer, S., & Doek, J. (2025). *TERMINOLOGY GUIDELINES FOR THE PROTECTION OF CHILDREN FROM SEXUAL EXPLOITATION AND SEXUAL ABUSE*.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103. https://doi.org/10.1080/17440572.2015.1013211

Hout, M. C. Van, & Bingham, T. (2013). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy*, *24*(6), 524–529. https://doi.org/10.1016/j.drugpo.2013.08.011

Huikuri, S. (2023). Users of Online Child Sexual Abuse Material. *Journal of Police and Criminal Psychology*, *38*(4), 904–913. https://doi.org/10.1007/s11896-023-09611-4

Humas KPAI. (2024). *Laporan Tahunan KPAI 2024, Jalan Terjal Perlindungan Anak: Ancaman Serius Generasi Emas Indonesia*.

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Ibrahim, D. (2022, May 12). *Online child sexual exploitation and abuse in Canada: A statistical profile of police-reported incidents and court charges, 2014 to 2020* . Juristat: Canadian Centre for Justice Statistics. https://www150.statcan.gc.ca/n1/ pub/85-002-x/2022001/article/00008-eng.htm

Inhope. (2022). *What is CSAM?* Inhope. https://www.inhope.org/EN/articles/what-is-csam

Inhope. (2024). *Annual Report 2024*.

Internet Watch Foundation. (2021). *Annual Reports 2021*. https://annualreport2021.iwf.org.uk/trends/darkwebreports

Internet Watch Foundation. (2024). *IWF Annual Data and Insights Report 2024.* . https://www.iwf.org.uk/annual-data-insights-report-2024/

Jenkins, P. (2001). *Beyond Tolerance: Child pornography on the internet.* New York University Press . https://www.ojp.gov/ncjrs/virtual-library/abstracts/beyond-tolerance-child-pornography-internet

Khera, V. (2020, November 2). Darkweb & Internet Anonymity: Exploring The Hidden Internet. *Cyber Protection Magazine*. https://cyberprotection-magazine.com/darkweb-internet-anonymity-exploring-the-hidden-internet

KPAI. (2021). *Data Kasus Perlindungan Anak 2016 – 2020*. https://bankdata.kpai.go.id/tabulasi-data/data-kasus-perlindungan-anak-2016-2020

Kusumawardhani, D. L. L. H. N., & Wulandari, S. (2024). *Strategy for Handling the Crime of Child Sexual Exploitation on the Era of Globalization by The State Police of The Republic of Indonesia (POLRI)*. 92–95. https://doi.org/10.2991/978-2-38476-325-2_11

Lavorgna, A., & Sergi, A. (2016). Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, *10*(2), 170–187. https://doi.org/10.5281/zenodo.163400/IJCC

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Livingstone, S., Carr, J., & Byrne, J. (2016). *OneinThree: InternetGovernance andChildren'sRights*. www.unicef-irc.org

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60. https://doi.org/10.1080/17440572.2012.759508

Maharani, N., Widagdo, S., Istiqomah, M., & Puspi-Tawati, D. (2026). Criminal Liability and the Non Punishment Principle for Trafficking Victims in Indonesia. *Jurnal IUS Kajian Hukum Dan Keadilan*, *14*. https://doi.org/10.29303/ius.v14i1.1820

Jurnal LITIGASI, Vol. 27 (1) April, 2026, p. 1-25
dx.doi.org/10.23969/litigasi.v27i1.43221

Mardin, N., Purnamasari, A. I., Miqat, N., Kharismawan, A., & Nur, R. (2022). Comparative Law Study: Sentencing of Sexual Violence Perpetrators Who have Deviant Sexual Behavior. *Jambura Law Review*, *4*(02), 227–245. https://tirto.id/komnas-perempuan-kasus-kekerasan-naik-2-kali-lipat-pada-2021-gmfy

Ministry of Justice. Home Office. (2025, July 1). *Crime and Policing Bill : Child Sexual Abuse Materials Factsheet*. Ministry of Justice. Home Office. https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-child-sexual-abuse-material-factsheet

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 71–80. https://doi.org/10.1145/2068816.2068824

National Centre of Missing or Exploited Children (NCMEC). (2024). *CyberTipline report* . https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf

Novianti, & Chusairi, A. (2024). Online Child Sexual Exploitation and Abuse (OCSEA) of Children and Adolescents: A Systematic Literature Review. *Psikologika : Jurnal Pemikiran Dan Penelitian Psikologi*, *29*(2), 281–306.

Nuridah, S., Nong, A. S., Ismail, N., Bin Mustaffa, A., Binti Bidin, A., & Taher, M. A. (2025). From Misbehaviour to Courtroom: Analyzing Malaysia's Legal Approach to Children Beyond Parental Control. *Jambe Law Journal*, *8*(2), 443–474. https://doi.org/10.22437/jlj.8.2.443-474

Office of Research-Innocenti. (2019). *Global Kids Online: Growing up in a connected world How do children's online experiences affect their rights and well-being?* https://www.unicef.org/innocenti/reports/global-kids-online-growing-connected-world

Owen, G., & Savage, N. (2015). *The Tor Dark Net*.

Rainn. (2025). *What is CSAM?* Rainn.Org. https://rainn.org/get-the-facts-about-csam-child-sexual-abuse-material/what-is-csam/.

Salter, M., & Mason, Julie. (2007). *Writing law dissertations : an introduction and guide to the conduct of legal research*. Pearson/Longman.

Santoso, L., & Musyayyadah, U. R. (2025). Challenging Legal Injustice against Children in Incest Cases: A Progressive and Islamic Human Rights Approach. *De Jure: Jurnal Hukum Dan Syar'iah*, *17*(2), 675–696. https://doi.org/10.18860/j-fsh.v17i2.36277

Savage, L. (2024). *Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022*. https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-eng.htm

Septianita, H., & Rachmie, S. (2024). Cyber Space: A Dangerous World for Children (Analysis on Transnational Online Child Pornography). *International Journal of Latin Notary*, *5*(1), 5–10. https://doi.org/10.61968/journal.v5i1.82

Simabura, C., Arinanto, S., Indrati, M. F., Isra, S., & Arsil, F. (2023). Ministerial Authority in Formulating Regulations Related to Presidential Lawmaking Doctrine. *Constitutional Review*, *9*(2), 297–331. https://doi.org/10.31078/consrev924

Suprapto, D. P., Faslukil, M., & Triyana, Y. (2023). Indonesia's Role in Preventing Transnational Cyber Pornography of Children in the Southeast Asian Region Viewed From a Political Law Approach. *International Journal of Social Science and Human Research*, *06*(06), 3871–3877. https://doi.org/10.47191/ijsshr/v6-i6-83

UNODC. (2014). *Protecting the Future: Responding to Child Sex Offending in Southeast Asia*. www.unodc.org

US Immigration and Customs Enforcement. (2014, January 15). *US Immigration and Customs Enforcement, 29 arrested in international case involving live online webcam child abuse*. US Immigration and Customs Enforcement. https://www.ice.gov/news/releases/29-arrested-international-case-involving-live-online-webcam-child-abuse,

van der Bruggen, M., & Blokland, A. (2021). Child Sexual Exploitation Communities on the Darkweb: How Organized Are They? In W. Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context* (pp. 259–280). Springer. https://doi.org/10.1007/978-3-030-60527-8_15

von Lampe, K. (2016). *Organized Crime*. SAGE Publications, Inc. https://doi.org/10.4135/9781506305110

von Lampe, K. (2026). Criminal network analysis and the study of organized crime*. *Global Crime*, 1–18. https://doi.org/10.1080/17440572.2026.2617567

Voziki, V. (2021). *Cyber-enabled child sexual exploitation and sexual abuse: Fighting for children's dignity and safety* . https://repository.ihu.edu.gr/xmlui/handle/11544/29851

We Protect Global Alliance. (2024). *Child Sexual Abuse Materials*. We Protect Global Alliance. https://www.weprotect.org/thematic/child-sexual-abuse-material/.