



ISSN 2985-0541 (Print) / ISSN 2539-5513 (Online)

JOURNAL OF CONTEMPORARY SOCIAL SCIENCES AND HUMANITIES

Available online at <https://jcs.h.rsu.ac.th>



Building an Integrated Enforcement Framework Against CSAM-Related Trafficking in Thailand

Thapana Bhasathiti Sanyabutra^{1,*}, Punchada Sirivunnabood¹, Veenunkarn Rujiprak¹, Seksan Khruakham², and Trynh Phoraksa¹

¹Faculty of Social Sciences and Humanities, Mahidol University, Nakhon Pathom 73170, Thailand

²Faculty of Social Sciences, Royal Police Cadet Academy, Nakhon Pathom 73110, Thailand

*Corresponding author; E-mail: thapana.san@student.mahidol.ac.th

Received 26 March 2026/ Revised 24 April 2026/ Accepted 6 May 2026/ Publish Online 7 August 2026

Abstract

This article develops an integrated enforcement framework for addressing human trafficking linked to the production and dissemination of child sexual abuse material (CSAM) in Thailand. The study employs documentary analysis; nine semi-structured in-depth interviews with officials from Thai and international law enforcement, prosecution, government, the private sector, and academia; and three focus group discussions (FGDs) involving law enforcement, prosecution, government agencies, and NGOs, totalling twenty-seven participation instances from twenty-one unique informants. Interviews and FGDs were guided by semi-structured, open-ended instruments. Findings indicate that the challenge is not the absence of legal provisions, but the misalignment of legal frameworks, institutional arrangements, and enforcement practices in responding to digitally mediated exploitation. Although the Palermo Protocol's act-means-purpose framework is formally applicable, cases are processed under CSAM or cybercrime offences rather than trafficking. This reflects institutional fragmentation, staff rotation, resource constraints, and performance indicators prioritising case volume and procedural efficiency over complexity and victim protection. The article proposes a four-pillar framework: centralised coordination and case screening; victim-centred pathways adapted to persistent digital harm; integrated digital intelligence and cross-border cooperation; and specialist capacity supported by performance reform. It realigns prosecution, protection, and prevention with child-rights-based principles and introduces mechanisms to identify and elevate exploitation within the trafficking framework. It advances a re-reading of trafficking in digital contexts, reoperationalises the three Ps for persistent digital harm, and integrates criminological and institutional perspectives. It concludes that effective enforcement requires institutional and operational reconfiguration centred on the rights and dignity of the child.

Keywords: *Child Sexual Abuse Material (CSAM), human trafficking, integrated enforcement framework, victim-centred approach, Thailand, online exploitation*

1. Introduction

Over the past decade, online child sexual abuse material (CSAM) has expanded rapidly at both global and regional levels, driven by the proliferation of high-speed internet, social media platforms, encrypted communication applications, and the dark web, which together facilitate the production, dissemination, and exchange of abusive content at scale (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2022). Forms of offending now extend beyond the recording of images or videos for possession to include live-streamed abuse, the coercion or inducement of children to produce sexual content, and sexual extortion (sextortion), reflecting the growing complexity of exploitation in digitally mediated environments (Açar, 2017; Martin & Alaggia, 2013; Napier et al., 2021).

Although CSAM encompasses the production, dissemination, possession, and viewing of material depicting child sexual abuse, not all CSAM cases constitute “human trafficking” within the meaning of the Palermo Protocol and Thailand’s anti-trafficking legislation (Blackburn et al., 2010; Davy, 2014). The relationship is one of partial overlap. Where the production, coercion of a child to produce, recording, or dissemination of CSAM occurs under conditions of control, deception, abuse of power, or exploitation of vulnerability for sexual exploitation or commercial gain, such conduct may, in certain contexts, satisfy the act-means-purpose elements of trafficking (Prasertsuk et al., 2019). By contrast, cases involving possession or viewing without exploitation in the production process are more appropriately addressed within CSAM or cybercrime frameworks.

Thailand has developed a substantial body of law and policy to address trafficking and child sexual abuse, including the Anti-Trafficking in Persons Act B.E. 2551 (ASEAN, 2008), legislation addressing CSAM-related offences, and the Computer-Related Crime Act B.E. 2550 (Ministry of Digital Economy and Society, 2007), alongside accession to the Palermo Protocol, the Convention on the Rights of the Child (CRC), and its Optional Protocols, and the ASEAN Convention Against Trafficking in Persons (ACTIP) (Blackburn et al., 2010; Johnson, 2014; Kranrattanasuit, 2014). Yet existing research consistently indicates that enforcement remains fragmented, reliant on agency discretion, and insufficiently integrated with anti-trafficking and child-rights standards (ECPAT, INTERPOL, & UNICEF, 2022; Thammasiri, 2024).

Empirical findings from interviews and focus group discussions indicate that practitioners frequently rely on CSAM or computer crime charges, even where cases exhibit indicators of control and exploitation consistent with trafficking (ECPAT, INTERPOL, & UNICEF, 2023; Mangkhalasiri et al., 2025). Such charges are often easier to establish through digital evidence without identifying victims or demonstrating broader structures of exploitation, whereas trafficking charges require greater resources and the activation of full victim protection measures (Mangkhalasiri, 2024; Thammasiri, 2024). Within institutions shaped by heavy workloads and performance metrics, reliance on CSAM charges may therefore become structurally rational, even where trafficking dimensions and victim rights are overlooked.

As a result, cases exhibiting trafficking characteristics are not consistently recognised or framed as trafficking. Children depicted in such material may therefore not be fully recognised or protected as trafficking victims, particularly in relation to non-punishment, access to services, and remedies. The core challenge lies not in the absence of legal provisions, but in the misalignment between legal frameworks, institutional structures, and enforcement practices in response to digitally mediated exploitation.

While trafficking, child sexual abuse, and cybercrime in Thailand have been widely studied, a specific gap remains in understanding the intersection between CSAM and trafficking and in developing empirically grounded enforcement approaches capable of addressing this phenomenon in digital contexts (Berger & van de Glind, 1999; Blackburn et al., 2010; Rafferty, 2007).

This article adopts a socio-legal and criminological perspective to examine how existing trafficking frameworks may be interpreted and operationalised in response to emerging forms of online CSAM-related exploitation. Drawing on qualitative analysis, criminological theory, and international legal frameworks, it analyses the structural, legal, and operational limitations of Thai agencies and develops an integrated enforcement framework linking prosecution, protection, and prevention through victim-centred, trauma-informed, and child-rights-based approaches.

The framework maintains the distinction between general CSAM and trafficking cases, while introducing mechanisms to systematically identify and elevate cases involving exploitation within a trafficking framework. It proposes an enforcement architecture that integrates structural, institutional, technological, and child-rights dimensions in order to strengthen both enforcement effectiveness and victim protection in line with international standards.

Section 2 sets out the conceptual framework and methodology. Section 3 identifies legal, institutional, and operational gaps. Section 4 presents the four pillars of the proposed framework. Section 5 demonstrates how the framework realigns the three Ps and victim-centred principles. Section 6 discusses policy implications and concludes.

2. Objectives

The objectives of this study are as follows:

- 1) To examine the legal, institutional, and operational gaps in Thailand's enforcement response to human trafficking linked to child sexual abuse material (CSAM).
- 2) To analyse the challenges faced by relevant enforcement and child protection actors in identifying, investigating, prosecuting, and protecting victims in CSAM-related trafficking cases.
- 3) To develop an integrated enforcement framework for CSAM-related trafficking in Thailand that aligns legal interpretation, institutional coordination, digital investigation, cross-border cooperation, and victim-centred protection.

3. Materials and Methods

3.1 Key Concepts and Theoretical Framework

The term "child sexual abuse material" (CSAM) refers to any visual, audio, or written depiction of a child engaged in real or simulated sexually explicit conduct, or any depiction of a child's sexual organs for primarily sexual purposes. Consistent with the terminology adopted by the Luxembourg Guidelines (Greijer & Doek, 2016), the Budapest Convention on Cybercrime, and the Lanzarote Convention, this definition encompasses not only traditionally produced images and videos, but also live-streamed abuse, coerced or self-generated sexual content, and digitally manipulated material (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2022).

The shift from the term "child pornography" to "child sexual abuse material" reflects a substantive conceptual reorientation rather than a purely semantic change. The term pornography may imply a degree of consensuality or legitimacy, which is fundamentally incompatible with the exploitation of children. By contrast, the use of CSAM foregrounds the abusive nature of the content and centres the victimhood of the child. This shift has been endorsed by international bodies, including the International Criminal Police Organization (INTERPOL) and ECPAT, and is increasingly reflected in national legislation and policy discourse (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2022).

The relationship between CSAM and human trafficking is commonly analysed through the act-means-purpose framework of the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Palermo Protocol), supplementing the United Nations Convention against Transnational Organized Crime. Under this framework, trafficking involves an "act" (such as recruitment, transfer, harbouring, or receipt of a person), undertaken through specified "means" (including coercion, deception, abuse of power, or exploitation of vulnerability), for the "purpose" of exploitation. The CRC and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography complement this framework by establishing that the best interests of the child shall be a primary consideration in all actions concerning children (Blackburn et al., 2010; Kranrattanasuit, 2014).

In cases involving children, the Palermo Protocol recognises that the "means" element need not be established. The recruitment, transfer, harbouring, or receipt of a child for the purpose of exploitation may constitute trafficking regardless of whether coercion or deception can be demonstrated. This principle is particularly relevant in CSAM contexts, where apparent consent may be shaped by age, developmental immaturity, grooming, or structural power imbalances (Blackburn et al., 2010; Rafferty, 2007).

Within this article, the relationship between CSAM and trafficking is understood as one of partial overlap. Not all CSAM-related conduct falls within the scope of trafficking. However, empirical and conceptual analysis suggests that certain cases involving the production or dissemination of CSAM may be associated with identifiable structures of control and exploitation. In this context, "structures of control and exploitation" refer to patterns such as coercion, deception, dependency, repeated production, or organised facilitation that sustain ongoing exploitation over time.

Accordingly, when examining CSAM-related conduct in digitally mediated environments, elements of the trafficking framework may, in certain contexts, be analytically extended to include forms of online recruitment through grooming, ongoing control exercised through digital coercion, or organised dissemination for sexual exploitation or commercial gain. These interpretations are advanced as analytical tools for understanding patterns of exploitation, rather than as definitive legal conclusions, and remain contingent on statutory frameworks and judicial interpretation (Blackburn et al., 2010; Rafferty, 2007).

A victim-centred and child-rights-based approach, as articulated in the Palermo Protocol, ACTIP, and the CRC, places the rights, needs, and dignity of victims at the centre of anti-trafficking responses, from identification and investigation through prosecution and recovery. In the context of CSAM, such an approach requires that children depicted in abuse material are recognised as victims rather than as witnesses or, in some cases, as participants in the production of illegal content (Piotrowicz & Sorrentino, 2016; Rafferty, 2007).

Central to this approach is the non-punishment principle, which holds that victims of trafficking should not be subjected to criminal penalties for unlawful acts committed as a direct consequence of their exploitation. In the CSAM context, this implies that a child who has been coerced or groomed into producing sexual images should not be treated as an offender for producing or possessing such material. The non-punishment principle is explicitly recognised in ACTIP and is increasingly regarded as an emerging norm in international practice (Piotrowicz & Sorrentino, 2016).

Theoretically, this article draws upon routine activity theory, which posits that crime occurs when a motivated offender converges with a suitable target in the absence of a capable guardian (Clarke, 1997), and situational crime prevention theory, which focuses on reducing criminal opportunities through environmental and situational interventions. These perspectives provide an analytical lens for understanding the structural conditions that facilitate the production and dissemination of CSAM, and for examining enforcement responses that address both individual offending and the broader opportunity structures that enable exploitation (Açar, 2017; Napier et al., 2021). Situational crime prevention is itself grounded in rational choice theory, which holds that offenders are purposive actors who weigh the perceived costs and benefits of an offence before acting (Cornish & Clarke, 1986). In the context of CSAM, the anonymity afforded by encrypted communications and the dark web, the geographic distance between offenders and victims, and the limited reach of guardianship across digital platforms distort this calculus. When the perceived benefits of exploitation, such as sexual gratification, financial gain, or status within offender networks, significantly outweigh the risk of detection and sanction, rational choice theory predicts that offending behaviour will persist. This theoretical lens reinforces the situational crime prevention argument that effective enforcement must alter the opportunity structures and risk perceptions that underpin offending decisions, rather than relying solely on punitive responses after the fact (Clarke, 1997; Cornish & Clarke, 1986).

In digitally mediated environments, these dynamics are particularly pronounced. Offenders may operate across jurisdictions, potential victims are widely accessible through online platforms, and guardianship is distributed across families, schools, technology companies, and state agencies, none of which exercises comprehensive oversight. The convergence of these elements creates persistent opportunity structures that differ qualitatively from those in physical environments (Broadhurst, 2019; Napier et al., 2021).

Beyond criminological theory, the study also draws upon institutional and governance perspectives to analyse how mandate fragmentation, siloed data systems, staffing practices, and performance metrics shape enforcement behaviour and constrain reform. These perspectives complement the criminological lens by directing attention to the organisational and bureaucratic conditions that mediate between legal frameworks and operational practice. In this regard, Herbert Packer's (1968) formulation of the crime control model and the due process model provides a further analytical tool. The crime control model prioritises efficient suppression of crime through swift arrest, prosecution, and punishment, treating the justice process as an assembly line oriented towards high-volume case throughput. The due process model, by contrast, emphasises the protection of individual rights and procedural fairness, even at the cost of reduced efficiency. The tension between these models is empirically manifest in the Thai enforcement context: institutional pressures to satisfy volume-based performance metrics, consistent with crime control logic, result in the systematic selection of narrower CSAM or cybercrime charges over the more resource-intensive trafficking framework, which demands a due-process-oriented approach to victim recognition and rights protection. An effective enforcement architecture must therefore manage and reconcile these competing imperatives rather than allowing efficiency pressures to displace victim-centred and due-process obligations (Packer, 1968). The rational-goal model further directs attention to the alignment of institutional performance indicators with desired outcomes, while the functional-systems model highlights the interdependencies among organisational subsystems and the need for coordination across institutional boundaries, both of which underpin the design of the four-pillar framework proposed in Section 4.

The discussion in this section is intended as an analytical and criminological interpretation of how trafficking frameworks may be applied in digitally mediated contexts. It does not seek to establish definitive legal interpretations, which remain subject to statutory frameworks and judicial determination.

3.2 Research Design and Ethical Approval

This study adopts a qualitative research design informed by grounded theory techniques, combining documentary analysis with semi-structured in-depth interviews and focus group discussions (FGDs). The use of iterative coding and the constant comparative method supports the development of analytical categories grounded in empirical data, and is particularly suited to examining under-researched areas in which existing frameworks may not fully capture the dynamics of trafficking in online environments (Davy, 2014; Martin & Alaggia, 2013).

The analysis is based on data from twenty-one informants drawn from justice and child protection agencies, international organisations, foreign government agencies, internet service and platform providers, and non-governmental organisations (NGOs). Sampling was guided by principles of analytical relevance and professional experience. Participants were required to have at least two years of service in their respective agencies and direct experience in law enforcement or policy responses related to trafficking or CSAM.

Nine semi-structured in-depth interviews were conducted with officials from the Office of the Attorney General, the Department of Special Investigation (DSI), the Cyber Crime Investigation Bureau (CCIB) and the Central Investigation Bureau (CIB) of the Royal Thai Police (RTP), the United States Homeland Security Investigations (HSI), the ASEAN-Australia Counter Trafficking Programme (ASEAN-ACT), the Ministry of Social Development and Human Security (MSDHS), a private-sector internet service provider, and a legal scholar specialising in crimes against children. Two FGDs, each comprising six participants, were conducted: the first included law enforcement officers from the Anti-Trafficking in Persons Division (ATPD), the Thailand Internet Crimes Against Children Task Force (TICAC), the Anti-Trafficking in Persons Center of the Royal Thai Police (TATIP RTP), the DSI, and the Department of Provincial Administration (DOPA); the second comprised government officials and NGO representatives. A third cross-cutting FGD of six participants drawn from the first two groups explored themes emerging across professional categories. Accordingly, while the total number of participation instances was twenty-seven, the number of unique informants remained twenty-one.

The qualitative sample size was determined based on principles of analytical saturation rather than statistical representation. Data collection continued until no substantially new themes emerged across interviews and FGDs, particularly in relation to institutional practices, legal framing, and operational constraints in CSAM-related trafficking cases. Interviews were conducted online using semi-structured, open-ended questions and were audio-recorded with participants' written informed consent.

The analytical process followed the constant comparative method associated with grounded theory. Interview and FGD recordings were transcribed verbatim and analysed through three stages of coding: open coding, identifying initial concepts; axial coding, exploring relationships among concepts; and selective coding, integrating core categories into a coherent analytical framework. The coding trajectory progressed from operational concerns (e.g. overlapping mandates, charge selection pressures, limited digital tools) through analytical categories (e.g. institutional fragmentation, evidentiary misalignment) to the development of four interdependent enforcement pillars. Documentary materials, including legislation, policy reports, case studies, and institutional guidelines, were analysed concurrently to contextualise and triangulate findings from primary data. The analysis was conducted in the original language and translated into English at the reporting stage, with back translation applied to key excerpts to ensure accuracy (Davy, 2014; Todres, 2010).

Ethical approval was obtained from the Mahidol University Social Sciences Institutional Review Board (MUSSIRB No. 2025/046; Certificate No. 2025/039.2904; approved 29 April 2025). All participants provided written informed consent prior to participation. Data were stored securely and anonymised during transcription and analysis to protect the identities of informants and any individuals mentioned in their accounts.

To enhance trustworthiness, the study employed methodological triangulation across documentary analysis, interviews, and FGDs, as well as data triangulation across participant categories, including law enforcement, prosecution, child protection, international organisations, and civil society. The iterative coding process ensured that findings remained closely grounded in participants' accounts while being interpreted through the conceptual framework of trafficking as exploitation (Davy, 2014; Todres, 2010).

Several limitations merit acknowledgement. First, the qualitative design prioritises depth over statistical generalisability; the findings reflect the perspectives of twenty-one institutional actors and are not intended to represent all agencies or jurisdictions. Second, participants were enforcement and policy professionals rather than survivors or children; the analysis therefore reflects an institutional perspective rather than lived experience. Survivor-centred participatory research would complement this approach in future work. Third, the online

interview format may have shaped the depth of disclosure on sensitive operational matters. Fourth, the article focuses on enforcement architecture rather than prevalence estimation, and the framework's applicability to other jurisdictions remains to be tested.

The analysis identified five recurring problem clusters: inconsistency between law and practice, institutional fragmentation, resource and capacity limitations, performance-indicator pressures, and obstacles to victim identification. These clusters, discussed in Section 3, inform the design of the four-pillar framework presented in Section 4. The framework is thus both empirically grounded in informants' accounts and analytically synthesised through the conceptual and theoretical perspectives outlined above (Davy, 2014; Todres, 2010).

3.3 International Approaches to CSAM-Related Enforcement: Comparative Perspectives

A review of enforcement models in selected jurisdictions provides important comparative context for the structural gaps identified in this article and for evaluating the framework proposed in Section 4. Three cases, namely the United States, the Philippines, and the United Kingdom, illustrate distinct but complementary institutional arrangements, and each of these arrangements addresses dimensions of CSAM-related enforcement that remain underdeveloped in Thailand's current response architecture.

In the United States, the National Center for Missing and Exploited Children (NCMEC) CyberTipline functions as a centralised national hub for receiving, triaging, and referring CSAM reports from both the public and online platforms (Popa, 2024). Platforms operating in the United States are legally required to report suspected CSAM to the CyberTipline, and federal specialist units, including the Department of Homeland Security Investigations (HSI) and the Federal Bureau of Investigation (FBI), coordinate on an intelligence-led basis. The Child Exploitation and Obscenity Section of the Department of Justice provides dedicated prosecutorial expertise, while the Internet Crimes Against Children Task Force Programme coordinates multi-agency responses at the state level. The result is a layered enforcement architecture in which standardised reporting, central triage, specialist investigation, and dedicated prosecution are structurally integrated (Shapiro, 2020).

Beyond these institutional arrangements, civil litigation in the United States has begun to develop a jurisprudence of platform accountability with direct implications for CSAM enforcement. In *P.F. et al. v. Meta Platforms, Inc. et al.* (Superior Court of California, County of Los Angeles, 2026), the first bellwether trial arising from the consolidated federal proceedings *In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation* (MDL No. 3047, N.D. Cal.), a jury found Meta and Google liable for defective platform design that caused psychological harm to a minor through addictive algorithmic features, awarding USD 6 million in compensatory and punitive damages. The MDL consolidates more than 10,000 individual cases and approximately 800 school district claims, proceeding on allegations that platforms deliberately engineered engagement-maximising features, including infinite scrolling, algorithmic content recommendation, and automatic video play, with knowledge of their harmful effects on minors, while concealing that knowledge from the public. Of more direct relevance to CSAM enforcement is *State of New Mexico ex rel. Torrez v. Meta Platforms, Inc. et al.* (New Mexico Courts, 2026). Following an undercover investigation in which state prosecutors created fictitious minor profiles and documented solicitation by predators, the jury found that Meta had violated the New Mexico Unfair Practices Act by misleading the public about the safety of its platforms, and that its recommendation algorithms had steered underage users towards sexually explicit content, CSAM, and sexual predators. The jury awarded USD 375 million in civil penalties, the maximum USD 5,000 per violation across thousands of identified contraventions, marking the first successful state lawsuit against Meta on child safety grounds (Hays, 2026; CNBC, 2026). Internal evidence introduced at trial indicated that Meta's 2019 decision to extend end-to-end encryption to Facebook Messenger was projected by its own staff to suppress approximately 7.5 million CSAM reports to law enforcement annually. Attorney General Torrez subsequently sought structural modifications to Meta's platforms, including age verification, removal of predators, and restrictions on encrypted communications that shield harmful actors. Taken together, these proceedings illustrate that civil accountability mechanisms are beginning to hold platforms liable not merely for hosting user-generated CSAM, but for the algorithmic and design decisions that create or amplify conditions of child sexual exploitation, a dimension of platform responsibility that Thailand's current enforcement frameworks have not yet engaged.

The Philippines provides an instructive model of legislative and institutional integration in a Southeast Asian context. Following the enactment of Republic Act No. 11930, the Anti-Online Sexual Abuse or Exploitation of Children Act (Republic of the Philippines: Philippines Commission on Women, 2022), the Philippines

established the National Coordination Centre against Online Sexual Abuse and Exploitation of Children (NCC-OSAEC), which serves as an inter-agency coordinating body mandated to develop gender-responsive, child-friendly, victim-centred, and trauma-informed protocols for responding to CSAM and online child exploitation. The legislation imposes 24-hour blocking obligations on internet service providers upon receipt of notice of CSAM content, mandates platform cooperation in detection and removal, and criminalises a broad range of conduct, including online grooming, live-streamed abuse, and AI-generated material. The legislative framework directly addresses the definitional and coordination gaps that impede enforcement in Thailand, while the NCC-OSAEC model closely parallels the centralised coordination function proposed in Pillar One of the framework developed in this article. The Philippines experience also demonstrates that classifying children who self-generate material as victims rather than offenders can be operationalised through legislative reform (International Centre for Missing and Exploited Children (ICMEC), 2022; Republic of the Philippines: Philippines Commission on Women, 2022).

In the United Kingdom, the Internet Watch Foundation (IWF) (2025) operates as a specialist hotline and analytical body working collaboratively with law enforcement, the technology industry, and government to detect, disrupt, and remove CSAM from the internet. The IWF maintains a hash list of confirmed CSAM that is shared with platform providers and used to prevent the upload and redistribution of known material (IWF, 2024). This collaborative governance model, in which a civil society body exercises a quasi-regulatory function in cooperation with public authorities and private platforms, redistributes the guardianship role across state and non-state actors. The Online Safety Act 2023 consolidates platform obligations further: under its illegal content duties, which entered into force in March 2025, all in-scope user-to-user and search services are legally required to assess the risk of CSAM on their platforms and to deploy hash-matching technology to detect and remove known CSAM, with enforcement conducted by the Office of Communications (Ofcom). Companies face fines of up to £18 million or ten per cent of qualifying worldwide revenue for non-compliance, and criminal liability may attach to senior managers in cases of serious breach. By April 2026, Ofcom had opened investigations into nearly 100 services, imposed multiple fines, and written directly to the six largest platforms, namely Facebook, Instagram, Roblox, Snapchat, TikTok, and YouTube, demanding evidence of further child safety improvements (IWF, 2024). At the supranational level, the European Union's Digital Services Act (European Union, 2022) establishes a risk-based regulatory architecture requiring very large online platforms to conduct systemic risk assessments, including risks from CSAM dissemination, and to implement proportionate mitigation measures subject to independent audit and enforcement by the European Commission. The EU is simultaneously negotiating a permanent Child Sexual Abuse Regulation, and in March 2026 the European Parliament endorsed a temporary extension of the ePrivacy derogation to allow continued voluntary detection of known CSAM in online communications until August 2027, pending agreement on a long-term framework (European Parliament, 2026). These regulatory architectures demonstrate that effective platform governance for CSAM suppression increasingly requires mandatory, enforceable, and technologically specific obligations rather than voluntary industry self-regulation.

These cases and regulatory frameworks illustrate that effective integrated enforcement responses share several structural features: centralised coordination and triage functions, mandatory platform reporting and content removal obligations, dedicated specialist capacity in investigation and prosecution, institutionalised public-private collaboration in digital intelligence, and, as the US litigation demonstrates, civil accountability for algorithmic decisions that facilitate exploitation. Each of these features is notably absent or underdeveloped in Thailand's current enforcement architecture. The comparative analysis thus reinforces the empirical findings presented in Section 3 and provides an international evidence base for the four-pillar framework proposed in Section 4.

4. Results

4.1 Diagnosing Legal, Institutional, and Operational Gaps

Although Thailand has enacted the Anti-Trafficking in Persons Act B.E. 2551 (ASEAN, 2008), the Computer-Related Crime Act B.E. 2550 (Ministry of Digital Economy and Society, 2007), Penal Code provisions concerning child sexual abuse materials, and the Child Protection Act B.E. 2546 (European Country of Origin Information Network, 2003), which together provide relatively broad legal coverage, the empirical findings indicate that structural weaknesses across several dimensions continue systematically to undermine law enforcement responses to trafficking linked to CSAM. The findings discussed in this section cluster around five

interrelated dimensions: inconsistency between law and practice, institutional fragmentation, limitations in resources and capacity, pressures arising from performance indicators and workload, and obstacles to victim identification.

4.1.1 Inconsistency Between Law and Practice

Findings from the interviews and FGDs indicate that one of the most significant structural problems lies in the gap between the legal framework and its practical enforcement. Practitioners operate across multiple overlapping legal regimes, including anti-trafficking legislation, computer crime law, and provisions relating to CSAM, with the choice of legal basis often shaped less by a structured assessment of facts through the act-means-purpose framework than by which agency first receives the case.

In practice, many cases are prosecuted solely under the Computer-Related Crime Act B.E. 2550 (Ministry of Digital Economy and Society, 2007) or CSAM offences, even where the facts reveal elements of control, grooming, and ongoing exploitation. This pattern suggests that CSAM is often treated primarily as a content offence, rather than as both a record and mechanism of sexual exploitation of children that may, in some contexts, engage the trafficking framework. As one prosecutor explained:

In practice, when we consider real cases, in many instances we rely principally on computer crime charges or child pornography offences because they are easier to prove than the elements of trafficking before Thai courts.

This reliance on offences with clearer and more easily provable elements produces a legal grey zone for trafficking linked to CSAM, in which victims do not receive full protection in accordance with victim-centred standards. The incomplete use of the trafficking framework has direct consequences for victim protection, because victims who are not recognised as trafficking victims cannot access the specific protection and assistance measures available to trafficked persons (Blackburn et al., 2010; Mangkhalasiri, 2024).

Interview evidence further indicates that evidentiary expectations remain tied to traditional conceptions of physical coercion, while digital evidence is not always interpreted in ways that support trafficking charges in CSAM cases. From the perspective of practitioners, this creates both evidentiary difficulty and legal risk, encouraging reliance on narrower offences that are perceived as easier to interpret and prove, even where they fail fully to capture the structure of exploitation (Martin & Alaggia, 2013).

This difficulty is reinforced by the statutory architecture itself. Under the Anti-Trafficking in Persons Act B.E. 2551 (ASEAN, 2008), prosecution requires proof that the accused committed an “act” (recruitment, transfer, harbouring, or receipt of a person), employed specific “means” (coercion, deception, abuse of power, or exploitation of vulnerability), and did so for the “purpose” of exploitation. In digital CSAM cases, however, the relevant conduct may involve online grooming through messaging applications, psychological coercion, or the exploitation of a child’s economic vulnerability-forms of conduct that do not fit neatly within evidentiary frameworks developed around physical trafficking. Several informants noted that prosecutors remain reluctant to advance trafficking charges in such cases because of uncertainty about how courts will interpret these digitally mediated manifestations of trafficking elements (Cullen et al., 2020; Mangkhalasiri, 2024).

This interpretive gap also shapes case routing at the initial stage. When a CSAM lead enters the system through the CCIB, the default pathway tends to follow the Computer-Related Crime Act B.E. 2550 (Ministry of Digital Economy and Society, 2007) or Penal Code provisions on obscene material rather than the Anti-Trafficking in Persons Act B.E. 2551 (ASEAN, 2008). Unless an officer has received specific training in identifying trafficking indicators within CSAM cases, the case is unlikely to be elevated. The result is a systemic undercount of trafficking cases and a corresponding failure to extend trafficking-level protection to child victims who might otherwise qualify (Mangkhalasiri et al., 2025; Thammasiri, 2024). This pattern of under-escalation is therefore not merely interpretive but structural, because it routinises the downgrading of exploitation into narrower offence categories and channels cases away from trafficking-based protection.

4.1.2 Institutional Fragmentation

Findings consistently indicate that another major structural gap lies in the fragmented institutional architecture governing trafficking linked to CSAM. Responsibilities are dispersed across numerous agencies, including the CCIB, TICAC, the ATPD (CIB), DOPA, the DSI, agencies under the MSDHS, child protection organisations, and various NGOs. While such dispersion reflects an intention to mobilise resources across sectors,

in practice the absence of a clearly designated case owner or central coordinating body creates significant discontinuities in enforcement.

Informants reported that when a lead or CyberTip from the National Center for Missing and Exploited Children (NCMEC) is received, referral decisions often depend more on personal relationships or prior experience than on formally prescribed terms of reference or standard operating procedures. At the same time, overlapping mandates among the ATPD (CIB), CCIB, TICAC, DSI, DOPA, and other agencies mean that the decision whether a case proceeds under a trafficking framework, a cybercrime framework, or child protection mechanisms is often made on a case-by-case basis rather than through a predetermined policy architecture (Kranrattanasuit, 2014; Mangkhalasiri, 2024).

The significance of this fragmentation is reflected in the fact that informants repeatedly called for a central coordinating mechanism for CSAM cases with trafficking elements, comparable to the Inter-Agency Council Against Trafficking in the Philippines (IACAT) or Thailand's Thai Maritime Enforcement Coordinating Centre (Thai-MECC). Their proposals suggest that this is not simply a matter of administrative convenience, but rather an institutional reform intended to reduce fragmentation and improve case continuity.

Data fragmentation forms a central part of this problem. Informants described how CyberTips from NCMEC, platform reports, NGO referrals, historical case data, suspect information, financial transaction trails, and records relating to child sex offenders are stored in separate agency silos, with no systematic integration. One law enforcement officer observed:

The data are stored separately. AMLO has the financial data, the police have case data, DSI has its own database. If they could be connected, we would see patterns of repeat offending and geographical hotspots. At present, we rely on personal networks to exchange information.

One TICAC officer noted, "When a CyberTip arrives, there is no automatic system to determine which agency should lead. It depends on who picks it up first, not on the nature of the case." This description is consistent with prior findings that inter-agency information-sharing systems remain a major weakness in Thailand's response to CSAM (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2022).

The absence of a unified case management system further compounds the problem. Each agency maintains its own record-keeping protocols, databases, and filing conventions, making it difficult to trace a case across its lifecycle, from the initial CyberTip or NGO referral through investigation, prosecution, and victim recovery. Informants reported that even within a single agency, information is often compartmentalised between units, requiring officers to rely on informal personal networks to obtain case-relevant data. This fragmentation reduces operational continuity, increases the risk of evidence loss and duplicated investigations, and creates gaps in victim protection during transitions between agencies (ECPAT, INTERPOL, & UNICEF, 2022; Mangkhalasiri, 2024). It also limits the system's analytical capacity to detect organised patterns of exploitation across agencies. Institutional fragmentation therefore operates not simply as a coordination failure, but as a structural condition that diffuses accountability and obstructs the recognition of trafficking patterns.

4.1.3 Limitations in Resources and Operational Capacity

The data also indicate that enforcement responses are constrained by significant limitations in resources and operational capacity. Informants repeatedly described systems of resource allocation and human resource management that are designed for ordinary cases rather than for complex, protracted, and specialist digital trafficking investigations.

These limitations include shortages of personnel, gaps in technical training, and budgetary constraints within agencies responsible for CSAM cases. Many officers function as generalists handling multiple categories of case, without a clear professional pathway as digital trafficking investigators or CSAM specialists. Those who do receive training in digital forensics, grooming and sextortion patterns, or trauma-informed approaches are often rotated through ordinary staffing systems, disrupting the accumulation of institutional knowledge and specialist expertise. One investigator remarked:

I was trained in digital forensics for six months, then rotated to a traffic division. The knowledge I built was simply lost.

In technological terms, informants reported that officers are sometimes required to monitor twenty to thirty online accounts simultaneously using manual methods, a practice widely regarded as unsustainable. This

suggests the need for automated tools and preliminary screening mechanisms, including hash-matching, keyword or behavioural detection, and risk-scoring systems, to identify high-risk cases before referral for in-depth investigation (Cullen et al., 2020).

These capacity constraints have cascading consequences across prosecution, protection, and prevention. In prosecution, the absence of long-term specialist investigative teams weakens the ability to sustain complex and cross-border investigations. In protection, the limited availability of personnel trained in both trauma-informed care and digital environments means that victim support is often confined to general child protection mechanisms. In prevention, the absence of permanent teams for digital intelligence, open-source intelligence (OSINT), and proactive monitoring means that these functions often remain temporary or project-based rather than institutionalised (Napier et al., 2021). Taken together, these deficits entrench a reactive model of enforcement in which proactive, intelligence-led responses remain aspirational rather than operational.

4.1.4 Pressures from Performance Indicators and Workload

Another recurring theme in the data concerns the influence of performance indicators and workload structures on enforcement behaviour. Although often treated as an administrative issue, participants described these pressures as highly significant in shaping investigative and charging decisions. Findings indicate that personnel systems and performance metrics are organised around short-term case cycles and annual budget cycles rather than around the lengthy and complex investigations characteristic of CSAM-related trafficking cases.

This structure weakens incentives to elevate cases to trafficking charges. Establishing the act, means, and purpose elements in digital contexts requires more time, more coordination, and greater evidentiary uncertainty than pursuing computer crime or CSAM offences, which can often be concluded more quickly and counted more readily towards performance targets. One child-protection official summarised the issue as follows:

If we speak frankly, when it comes to enhancing law enforcement effectiveness against trafficking in the form of CSAM, the primary indicators should not simply be the number of cases or suspects. We must ask whether every child victim was properly identified, whether they received safe protection, and whether our system prevented them from being re-victimised within the justice process.

Viewed through institutional and governance perspectives, this pattern suggests that existing performance frameworks do not merely measure outcomes but actively shape enforcement behaviour. Project-based training models that prioritise the number of participants, rather than sustained professional pathways and competency certification, further inhibit the accumulation of institutional capital necessary for the long-term handling of CSAM cases (Johnson, 2014; Mangkhalasiri, 2024).

From the victim perspective, these same workload and staffing structures also undermine the capacity to build sustained relationships of trust with child victims, which is central to trauma-informed practice. Staff rotation and heavy caseloads make continuity difficult, even where practitioners are committed to child protection. In effect, the current system structurally rewards undercharging and short-term efficiency, while disincentivising the elevation of cases that the trafficking framework is intended to capture. Performance-indicator structures therefore do not simply reflect institutional priorities, but help produce them.

4.1.5 Obstacles to Victim Identification and the Risk of Secondary Victimization

The gap with the gravest consequences for children concerns obstacles to victim identification and the risk of secondary victimisation within the justice process. Findings indicate that some children trafficked through CSAM are neither identified nor formally recognised as trafficking victims, and are therefore unable to access the specific protection measures available under Thai law and ACTIP, including specialised witness protection, shelter and long-term rehabilitation, legal assistance, and compensation.

Participants also described a victim protection system that still tends to position children as witnesses in pornography or cybercrime cases rather than as trafficking victims experiencing continuing harm from the persistence of CSAM in digital environments. Several informants observed that some officials continue to question children in ways that imply personal responsibility, for example, “Why didn’t you refuse?”, “Why did you agree to take the photographs?”, or “Did you know this was wrong?” For children who have been groomed over a long period or controlled through unequal power relations, such questions may reinforce shame and self-

blame rather than recognition of victimhood. This pattern constitutes a form of secondary victimisation within the justice process (Piotrowicz & Sorrentino, 2016; Rafferty, 2007).

One child-protection official observed:

Some children do not even know they are victims. They believe they chose to send the images.

Our system reinforces that belief instead of correcting it.

The findings also underscore the importance of persistent digital harm. Unlike physical crimes in which harm may be temporally bounded by the duration of the offence, CSAM may continue to circulate indefinitely in digital environments. Each act of viewing, sharing, or redistribution can therefore reproduce a renewed violation of dignity and privacy. Informants described cases in which children reported ongoing anxiety, sleep disturbance, and social withdrawal years after the initial abuse had ended, driven by the knowledge, or fear, that their images remained accessible online. This continuing harm challenges assumptions that the consequences of crime are finite and temporally bounded, and points to the need for protection mechanisms that extend beyond the conclusion of criminal proceedings (ECPAT, INTERPOL, & UNICEF, 2023; Martin & Alaggia, 2013).

A related gap concerns the absence of a formal notification mechanism. At present, there is no system in Thailand through which child victims are informed whether platforms have complied with requests to remove their images. Several informants noted that this leaves victims in a state of ongoing uncertainty regarding the continued circulation of their material. It also leaves agencies without a systematic means of verifying whether content removal has in fact occurred, weakening both victim recovery and the assessment of platform cooperation. Establishing a victim notification system linked to a central coordination mechanism would be one possible step towards addressing this protection gap (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2023).

In relation to rehabilitation, informants indicated that the current system continues to focus largely on temporary shelters or welfare centres. After a designated period, children return to their families or original communities, which may themselves be marked by violence, poverty, or substance abuse. In the absence of sustained educational and economic rehabilitation measures, the risk of renewed exposure to exploitative environments remains high (Davy, 2014; Prasertsuk et al., 2019).

Viewed collectively, the five gaps analysed in this section - inconsistency between law and practice, institutional fragmentation, resource limitations, performance-indicator pressures, and obstacles to victim identification - do not operate as isolated problems. Rather, the findings suggest an interconnected system of structural constraints in which each dimension reinforces the others. An enforcement architecture designed primarily for crime in physical environments continues to shape responses to digitally mediated exploitation, leaving the suppression of CSAM-related trafficking fragile across all dimensions of prosecution, protection, and prevention. These findings provide the empirical basis for the enforcement architecture outlined in the following section.

4.2 Core Pillars of the Integrated Enforcement Framework

Building on the findings presented in Section 3, this article outlines an integrated enforcement framework for responding to trafficking linked to CSAM in Thailand. The framework comprises four interrelated pillars that connect prosecution, protection, and prevention with victim-centred approaches, trauma-informed practice, digital intelligence, and institutional reform in the context of exploitation in online environments. These pillars are not discrete proposals but components of a mutually reinforcing system.

4.2.1 Pillar One: Centralised Mandate and Coordination for CSAM-Related Trafficking

Findings from the interviews and FGDs indicate that one of the principal obstacles in responding to CSAM cases with trafficking elements is the overlap of mandates among multiple agencies, including the ATPD (CIB), the CCIB, TICAC, the DSI, DOPA, and child protection agencies, without any clearly designated lead body for each category of case. As discussed in Section 3, this situation results in case screening, resource allocation, and prosecution being conducted on an ad hoc basis rather than through a clearly structured system (Kranrattanasuit, 2014; Mangkhalasiri, 2024).

In response to this gap, the framework centres on the establishment or upgrading of a central coordination hub for CSAM cases with trafficking elements. The proposed hub would have a clear mandate to: (1) assume case ownership and determine case routing according to the act-means-purpose framework; (2) manage an integrated database combining CyberTips from NCMEC, reports from platforms, NGO referrals, OSINT, and domestic case

data; and (3) serve as the central coordination point among the ATPD (CIB), CCIB, TICAC, the DSI, child protection agencies, specialist prosecutors, NGOs, and international partners.

This approach is consistent with comparative models in other jurisdictions, such as the NCMEC CyberTipline, which functions as a central information and referral hub across agencies (Popa, 2024), and specialist units such as HSI and the Federal Bureau of Investigation (FBI), which operate on an intelligence-led basis (Shapiro, 2020). In the context of this article, the purpose of the hub is to reduce institutional fragmentation, clarify the roles of lead and supporting agencies, and shift enforcement from a reactive model focused on isolated cases towards a more intelligence-led model capable of identifying patterns and networks (ECPAT, INTERPOL, & UNICEF, 2022).

In operational terms, informants described such a hub as maintaining a shared digital dashboard integrating CyberTips from NCMEC, platform reports, OSINT, financial intelligence from the Anti-Money Laundering Office (AMLO), and domestic case data. As one DSI investigator put it:

If we had a single dashboard showing all CSAM tips, financial trails, and case histories together, we would catch networks, not just individuals.

Upon receiving a CSAM-related lead, the hub would apply the act-means-purpose screening framework to assess whether the case presents indicators of trafficking. Cases meeting the threshold would be elevated to the trafficking track and assigned to a specialist multidisciplinary team, whilst cases assessed as falling within the general CSAM framework would be referred to the appropriate cybercrime unit. This triage function, which is absent from the current system, would help ensure that cases with trafficking characteristics are not overlooked simply because they enter the system through a cybercrime channel (Popa, 2024; Shapiro, 2020).

This pillar therefore addresses the coordination and screening problems identified in Section 3. While it is institutionally linked to the digital intelligence infrastructure and offender database discussed under Pillar Three, its primary function is to establish a central mandate, structured case routing, and continuity of case ownership.

4.2.2 Pillar Two: Digital-Era Victim-Centred and Trauma-Informed Pathways

The second pillar responds to the findings in Section 3 concerning obstacles to victim identification and the risk of secondary victimisation. It places the victim pathway, from first contact through to longer-term recovery, at the centre of the proposed architecture and adapts that pathway to the persistent digital harm associated with the continued existence and circulation of CSAM online, which may cause victims to experience the abuse as ongoing rather than concluded (Martin & Alaggia, 2013). In this respect, the pillar departs from the case closed–harm ended logic that continues to shape many justice systems.

The principal elements of this pillar include a victim identification system that treats CSAM cases as trafficking cases where structures of control and exploitation are present, even in the absence of physical movement or traditional forms of overt coercion; operational standards limiting repeated testimony through a single-interview, multiple-use approach together with child-friendly facilities; file-management mechanisms that prioritise safety, privacy, and dignity, including the use of hash-matching instead of repeated viewing of images; and longer-term support for victims suffering persistent digital harm, including assistance with content removal and access to psychosocial services throughout the life course (Piotrowicz & Sorrentino, 2016; Rafferty, 2007).

Importantly, this framework does not seek to treat every CSAM case as a trafficking case. Rather, it calls for clear legal and operational criteria so that cases involving the production, coercion of a child to self-produce, recording, or systematic dissemination of CSAM within an exploitative structure are consistently screened and, where appropriate, escalated into the trafficking process. This requires greater alignment among anti-trafficking law, child protection law, cybercrime law, and evidentiary law, together with the development of guidance enabling practitioners to determine when a case warrants elevation from general CSAM charges to the trafficking framework (Blackburn et al., 2010; Johnson, 2014).

This pillar is therefore intended to address not only recognition gaps in victim identification, but also the protection consequences that follow when victims are processed primarily through pornography or cybercrime frameworks rather than through trafficking-based responses. In that sense, it translates the victim-centred and child-rights-based principles discussed in Section 2 into an operational pathway suited to digitally mediated exploitation.

4.2.3 Pillar Three: Integrated Digital Intelligence, Cross-Border Cooperation, and Platform Engagement

The third pillar responds to the resource, capacity, and coordination problems identified in Section 3 by emphasising that the suppression of CSAM linked to exploitation cannot rely solely on reactive domestic law enforcement. Instead, it requires an integrated digital intelligence infrastructure, structured cross-border cooperation, and sustained engagement with digital platforms. While Pillar One establishes the institutional hub and screening mechanism, this pillar addresses the technological and transnational capacities through which that hub would operate.

This pillar is organised around three interrelated components. The first is the establishment of an integrated digital intelligence system combining CyberTips, NCMEC referrals, platform reports, and NGO information into a shared tool for proactive monitoring, OSINT, and hash-matching. The second is the systematic use of international cooperation mechanisms, including mutual legal assistance (MLA), joint investigations, and police-to-police channels, within the frameworks of the Palermo Protocol and ACTIP, rather than continued reliance on informal personal networks (Broadhurst, 2019). The third is the clarification of the roles and responsibilities of platforms and internet service providers in detecting, reporting, preserving, and removing CSAM, thereby redistributing responsibility from victims and the State towards private actors that exercise significant control over digital infrastructures. Informants identified several relevant operational levers, including possible mandatory reporting obligations for platforms operating in Thailand, standardised hash-sharing protocols with NCMEC and INTERPOL, expedited preservation orders for digital evidence, and designated law enforcement contact points within major platform providers.

This pillar is consistent with routine activity theory, which posits that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge, and with situational crime prevention theory, which emphasises reducing criminal opportunities through environmental design (Clarke, 1997). In digitally mediated environments, this means reshaping opportunity structures and strengthening guardianship through platforms and institutional systems, rather than placing responsibility on the behaviour of victims (Napier et al., 2021).

A further component of this pillar is a restricted, role-based database of CSAM-related child sex offenders, maintained under the central coordination hub as one safeguarding mechanism within the proposed architecture. This measure is advanced cautiously as a possible safeguarding tool, subject to strict legal scrutiny, necessity, and proportionality, and designed in compliance with child-rights and data protection principles. Such a database would connect CyberTips, case and judgment data, prison and probation information, and screening systems for individuals working in close proximity to children. Informants from law enforcement and child protection agencies expressed support for a managed offender data system, while also emphasising that its value depends on strict governance and clearly limited scope. The proposed instrument is not a public registry but a restricted safeguarding mechanism governed by a child-rights-based data governance framework with clearly defined rules on access, retention periods, independent oversight, and appeal mechanisms. Access would be limited to authorised personnel on a role-based basis, with retention periods prescribed by law and subject to periodic review and deletion where the individual no longer presents a demonstrable risk. Without such safeguards, there is a risk that the database could evolve into a punitive instrument that undermines the rights it is intended to protect rather than functioning as a proportionate and effective tool for child safeguarding (Cullen et al., 2020; Sharapov et al., 2024).

In this respect, this pillar addresses the operational reality that trafficking linked to CSAM is digitally mediated, transnational, and platform-dependent. It therefore supplies the intelligence, cooperation, and platform-governance capacities necessary for the broader framework to function in practice.

4.2.4 Pillar Four: Sustainable Specialist Capacity and Institutional Performance-Indicator Reform

The fourth pillar addresses the findings in Section 3 concerning resource constraints, workload pressures, staff rotation, and performance-indicator structures. Without changes in institutional design, including performance indicators, career pathways, and budget structures, the first three pillars would remain fragile, temporary, and project-based rather than sustainable (Sharapov et al., 2024).

The principal components of this pillar include the reform of performance indicators so that they measure the quality of suppression and victim protection in CSAM cases with trafficking elements, rather than merely the number of cases or the speed of closure. In this context, revised indicators would reward efforts to screen and

elevate CSAM cases containing trafficking elements instead of encouraging rapid closure under narrower offences (Prasertsuk et al., 2019; Todres, 2010). A second component is the creation of clear career pathways for digital trafficking investigators, digital forensic officers, specialist prosecutors, and child protection officials working on CSAM, thereby preserving and accumulating institutional memory over time rather than losing it through routine staff rotation (Davy, 2014; Thammasiri, 2024). A third component is the conversion of internationally funded temporary tools and positions into permanent posts and state budget lines in order to reduce the dependency trap that undermines continuity in enforcement.

In the prevention dimension, institutional and performance-indicator reform could also extend to migrant labour management systems and work permit regimes by linking them more explicitly to child protection and trafficking prevention objectives. One possible pathway would be to require foreign nationals applying for occupations involving close contact with children to produce criminal record checks from their countries of origin. Such measures reflect the broader argument that the prevention of CSAM-related trafficking cannot be confined solely to the criminal justice system but may also extend into the policy boundaries of labour regulation and education (ECPAT, INTERPOL, & UNICEF, 2023; Mangkhalasiri et al., 2025).

A critical dimension of sustainability concerns the transition from internationally funded pilot programmes to domestically financed permanent functions. The empirical data indicate that several key capabilities, including digital forensic equipment, specialist training programmes, and victim support coordinators, are currently funded through time-limited international cooperation projects. When project funding expires, these capabilities are frequently discontinued, and personnel who acquired specialist skills during the project period are reassigned to unrelated duties. This cycle of capacity building followed by capacity loss undermines institutional memory and prevents the consolidation of expertise. The fourth pillar therefore proposes that the national budget allocate dedicated line items for CSAM-related trafficking enforcement, ring-fenced from general police and prosecution budgets, and subject to outcome-based performance review rather than annual expenditure targets. Combined with the career pathway and performance-indicator reforms outlined above, such budgetary reform would help create the institutional conditions necessary for sustainable enforcement capacity (Johnson, 2014; Sharapov et al., 2024).

Taken together, the four pillars, namely centralised mandate and coordination, rights-based victim protection pathways adapted to online environments, integrated digital intelligence and cross-border cooperation, and specialist capacity combined with performance-indicator reform, are best understood not as isolated proposals but as components of an enforcement architecture designed to respond systematically to the structural gaps diagnosed in Section 3. The following section shows how this model realigns the three Ps and victim-centred principles in practice.

5. Discussion

5.1 Re-Aligning the Three Ps and Victim-Centred Principles

The proposed architecture does not merely append additional components to the three Ps framework. Rather, it realigns prosecution, protection, and prevention so that these dimensions operate more consistently with victim-centred, child-rights-based, and trauma-informed principles within a redesigned enforcement structure. This section examines how the four pillars reshape each of the Ps, focusing on the analytical shifts involved rather than restating the operational details of the framework.

5.1.1 Prosecution: Institutionalising Screening to Resolve the Efficiency–Justice Tension

In the prosecution dimension, the central analytical shift lies in addressing the tension between prosecutorial efficiency and victim-centred justice. As discussed in earlier sections, reliance on CSAM or cybercrime charges is structurally rational within the current system because such charges are generally easier to prove and more readily satisfy performance targets. The proposed framework responds to this tension not by expecting individual officers to exercise greater diligence, but by institutionalising the screening function. Under this model, a designated coordination hub would apply the act-means-purpose framework systematically to incoming cases, reducing reliance on individual discretion and embedding charge elevation within a structured organisational process (ECPAT, INTERPOL, & UNICEF, 2022; Shapiro, 2020).

This shift is significant because it weakens the link between performance-indicator pressure and charge selection. Prosecutors operating within the hub's referral structure would receive cases that had already been

screened for trafficking elements, thereby reducing the legal and evidentiary uncertainty associated with advancing trafficking charges and providing a documented rationale for doing so. When combined with digital-era victim protection pathways, this structure also enables prosecutorial decisions to account more fully for secondary victimisation and persistent harm, including the reduction of repeated file viewing, stronger protection of personal data, and greater victim participation in decisions concerning the use of their images, in line with the Palermo Protocol and ACTIP (Piotrowicz & Sorrentino, 2016; Rafferty, 2007). In this respect, the framework shifts charge selection from an individual discretionary act to an institutionalised process that is better aligned with both evidential realities and victim-centred justice.

5.1.2 Protection: From Episodic Intervention to Ongoing Digital Harm Management

In the protection dimension, the key analytical shift is the movement from episodic, case-based intervention to the ongoing management of persistent digital harm. Conventional protection frameworks tend to treat the conclusion of criminal proceedings as the endpoint of the State's protective obligation. The proposed architecture departs from that assumption by recognising that CSAM may persist indefinitely in digital environments, and that each act of redistribution may constitute a renewed violation of dignity and privacy (Martin & Alaggia, 2013). Extending protection beyond the lifespan of a single case, through longer-term recovery support, digital file management, and victim notification mechanisms, therefore reflects a redefinition of protection in digitally mediated contexts.

Recognising that CSAM cases containing exploitative structures may fall within the trafficking framework also opens access to the stronger protection regime available under trafficking law, ACTIP, and the CRC, including non-punishment, access to services, and specialised remedies, for victims who currently remain outside that regime (Johnson, 2014). In practice, this requires justice processes and file-management systems to be designed in ways that reduce re-traumatisation and increase victims' control over their images, for example through hash-based identification and support for online content removal. Such measures reflect the reality that pre-digital victim-centred principles are insufficient where harm continues through file circulation long after the initial abuse (Broadhurst, 2019; ECPAT, INTERPOL, & UNICEF, 2023). Protection is thus re-conceptualised not as a temporally bounded response to a completed event, but as an ongoing obligation shaped by the persistence of digital harm.

5.1.3 Prevention: From Awareness Campaigns to Structural Opportunity Reduction

In the prevention dimension, the framework shifts emphasis from behavioural awareness campaigns aimed at children and families towards structural opportunity reduction through platform governance and environmental design. This reflects the application of situational crime prevention theory: rather than focusing primarily on changing the behaviour of potential victims, the framework seeks to reshape the opportunity structures within which offending occurs (Clarke, 1997). Platform engagement mechanisms, hash-matching systems, and proactive OSINT monitoring extend the concept of the capable guardian to include private actors and specialist digital investigative teams, consistent with routine activity theory (Açar, 2017; Napier et al., 2021).

Performance-indicator reform reinforces this structural approach by incorporating preventive indicators that reward proactive monitoring and case elevation rather than volume-based closure. In doing so, it helps ensure that structural prevention is institutionally incentivised rather than dependent on the initiative of individual officers or temporary project teams (Cullen et al., 2020; Sharapov et al., 2024). Prevention is therefore no longer conceived primarily as behavioural modification, but as the restructuring of opportunity environments in which institutional design and platform governance become central to reducing exploitation risks.

These realignments also reveal a set of tensions that should be acknowledged rather than obscured. Prosecutorial efficiency may conflict with the time and care required for victim-centred case preparation. Platform governance requires regulatory and technical capacity that may exceed the current reach of Thai enforcement institutions. The specialist investment required across all four pillars may also sit in tension with the bureaucratic rotation cultures identified in Section 3. The proposed framework does not eliminate these tensions. Rather, it provides an institutional architecture within which they may be managed more transparently and equitably (Blackburn et al., 2010; Todres, 2010).

5.2 Policy Implications

The integrated enforcement framework developed in this article is best understood as an analytical and normative model rather than an operational blueprint capable of immediate implementation. Its application therefore depends upon adaptation to Thailand's institutional, legal, and political context.

In terms of legal reform, the findings suggest that enhancing enforcement effectiveness is less a matter of creating new offences or increasing penalties than of ensuring that existing legal frameworks are capable of addressing trafficking in digitally mediated contexts through child-rights-based approaches. This includes consideration of how the Anti-Trafficking in Persons Act, computer crime law, the Child Protection Act, and relevant criminal provisions may be better aligned to clarify the relationship between exploitation through CSAM and trafficking. It also involves the continued shift from the terminology of child pornography to that of CSAM, and clarification that the production, recording, and dissemination of CSAM within structures of control and exploitation may, in certain contexts, fall within the act-means-purpose framework, even in the absence of physical movement (Kranrattanasuit, 2014; Piotrowicz & Sorrentino, 2016).

In institutional terms, the findings point to the importance of a central coordination function for CSAM cases with trafficking elements, with the capacity to screen cases using the act-means-purpose framework and the three Ps, to manage and analyse data from CyberTips, NCMEC, NGOs, and OSINT, and to coordinate systematically across domestic agencies and international partners. This may also involve consideration of a restricted national database of child sex offenders linked to CSAM cases under the governance of such a coordinating mechanism (Mangkhalasiri, 2024; Popa, 2024).

At the operational level, the analysis highlights the need for more integrated procedures for handling CSAM cases with trafficking elements. This includes the development of national SOPs that connect the process from initial report, screening, and preservation of digital evidence through investigation, inter-agency referral, and victim protection within a single pathway. Such procedures would incorporate principles such as single interview–multiple use, child-friendly facilities, and limiting file viewing to what is strictly necessary, in order to reduce re-traumatisation (ECPAT, INTERPOL, & UNICEF, 2023; Mangkhalasiri et al., 2025).

An emerging challenge that the framework must also take into account is the proliferation of AI-generated CSAM. Advances in generative artificial intelligence have made it possible to create realistic synthetic images depicting child sexual abuse without the involvement of a real child. This development presents a number of challenges for existing enforcement approaches: hash-matching technologies may be less effective in detecting novel AI-generated content, legal definitions premised on the involvement of a real child may not fully capture synthetic material, and the volume of such content may place additional pressure on detection systems. The framework therefore requires sufficient adaptability to respond to these developments, including the potential use of AI-based detection tools and consideration of how legislation addresses AI-generated CSAM (Broadhurst, 2019; Cullen et al., 2020).

With regard to sequencing, the findings suggest that implementation may, subject to legal and administrative feasibility, proceed in phases. An initial phase could focus on establishing a central coordination hub on a pilot basis, deploying integrated digital intelligence systems, and developing a restricted offender database on a limited scale within selected provinces, alongside the conclusion of inter-agency memoranda of understanding to formalise data-sharing arrangements. A subsequent phase could address the harmonisation of relevant legislation, the development of specialist career pathways and professional certification for digital trafficking investigators, and the reform of performance indicators to prioritise case quality, victim identification, and appropriate charge selection. A phased approach of this kind would allow for iterative learning and adjustment, while reducing the risks of institutional resistance and resource overstretch (Davy, 2014; Sharapov et al., 2024; Thammasiri, 2024).

A recurrent finding across informant accounts that merits explicit policy attention is the tendency of government officials to underestimate the urgency and significance of CSAM-related trafficking cases. This underestimation arises not from indifference alone, but from the complexity of the legal framework and the cumbersome procedural requirements involved in prosecuting offenders and delivering care and rehabilitation to victims. When enforcement processes are perceived as overly burdensome, agencies default to simpler legal pathways, such as cybercrime charges, in ways that systematically deprioritise victim protection. This pattern is analogous to how labour trafficking is often pursued only as labour fraud, reflecting institutional habits of framing exploitation in its narrowest available legal category.

The empirical findings reinforce the argument that effective law enforcement in CSAM-related trafficking cases cannot rest primarily on harsher penalties or increased statutory severity. As informants emphasised, enforcement effectiveness must begin with a fundamental shift in understanding, mindset, and attitudes among officials at all levels, including senior leadership. This shift requires that officials recognise CSAM not merely as illegal digital content, but as a record of violence against children and a mechanism through which exploitation is produced, extended, and reproduced across digital environments. Authorities should therefore adopt proactive approaches to victim identification and offender detection, rather than waiting for cases to enter the system through the narrowest available channel, and should ensure the timely arrest and prosecution of offenders in ways that preserve victim protection standards throughout the process (Cornish & Clarke, 1986; Packer, 1968).

This attitudinal transformation also has implications for legal reform. Existing definitions of human trafficking and related offences may require revision to better reflect the realities of digital exploitation, including the use of artificial intelligence to generate synthetic CSAM that depicts or simulates children. From a rational choice theory perspective, enforcement strategies must ensure that offenders perceive no meaningful benefit from engaging in CSAM-related activities, whether by reducing opportunity structures, strengthening detection mechanisms, or increasing the certainty of sanction (Clarke, 1997; Cornish & Clarke, 1986).

Finally, the findings highlight the need for sustained, serious, and institutionally embedded investment in digital forensics capacity. The rotation of trained personnel out of specialist roles, and the dependency on time-limited international funding for digital forensic equipment and expertise, create a structural vulnerability that undermines the entire enforcement architecture. Digital forensics is not an ancillary technical support function but a core component of the investigative and prosecutorial process in CSAM-related trafficking cases. Building and retaining specialist capacity in this area, through dedicated career pathways, protected budget lines, and ongoing professional certification, is therefore a prerequisite for the realisation of the framework's prosecution and prevention pillars.

6. Conclusion

This article began from the proposition that the online production and dissemination of child sexual abuse material in Thailand continues to be addressed primarily as pornography or cybercrime rather than being recognised as a form of trafficking where an exploitative structure is present. Through analysis of empirical findings from in-depth interviews and FGDs, interpreted through criminological theory, human rights frameworks, and comparative international perspectives, the article has shown that this problem does not lie at the level of individual officials. Rather, it emerges from the interaction between pre-digital legal interpretations, fragmented institutional arrangements, and resource and performance systems that remain misaligned with digital crime and children's rights.

The proposed architecture consists of four interrelated pillars: centralised mandate and coordination, victim-centred protection pathways adapted to the digital context, integrated digital intelligence and cross-border cooperation, and sustainable specialist capacity combined with performance-indicator reform. These pillars are best understood not as isolated proposals, but as components of an enforcement architecture that realigns prosecution, protection, and prevention with victim-centred and trauma-informed principles in response to exploitation in online environments.

At the theoretical level, the article offers three contributions. First, it advances an analytical re-reading of the trafficking act-means-purpose framework in digitally mediated contexts, suggesting that the production and dissemination of CSAM within structures of control and exploitation may, in certain circumstances, fall within the scope of trafficking, even in the absence of physical movement. Second, it reoperationalises the three Ps and child-centred principles for online environments characterised by persistent digital harm, transnational offender networks, and platform-governed systems. Third, it integrates criminological theory, including routine activity theory, rational choice theory, and situational crime prevention, with institutional and governance perspectives, including criminal justice administration models, to develop an enforcement architecture that addresses not only individual offending but also the structural and institutional conditions that enable exploitation to persist (Blackburn et al., 2010; Clarke, 1997; Cornish & Clarke, 1986; Packer, 1968; Todres, 2010).

At the policy level, the analysis points towards the importance of institutional and legal reform, including the potential role of a restricted database of sex offenders linked to CSAM cases as one component within a

broader enforcement architecture. Such a measure is understood as part of a wider system connecting digital intelligence, child protection, and the prevention of repeat offending, and must be designed within a clear human rights and child-rights framework (Cullen et al., 2020; Napier et al., 2021).

More broadly, the findings underline that CSAM should not be understood merely as illegal content, but as a record of violence inflicted upon children and a mechanism through which sexual exploitation may be extended and reproduced across borders. Enhancing the effectiveness of anti-trafficking law enforcement in cases involving the online production and dissemination of CSAM in Thailand therefore cannot be assessed solely by reference to case numbers or severity of punishment. Rather, it depends upon the extent to which legal frameworks, institutional arrangements, power relations, and technological systems are reoriented around the dignity and rights of the child.

Future research may usefully test, apply, and compare the enforcement framework developed in this article across jurisdictions, particularly within Southeast Asia where similar contextual conditions exist. Quantitative and comparative analysis of offending patterns, institutional responses, and the effects of legal and policy interventions, together with ethically grounded participatory research involving victims and survivors, would further refine and extend the framework. In this respect, the analysis offered here contributes to ongoing efforts to strengthen responses to trafficking in digitally mediated contexts in ways that are both effective and consistent with the rights and lived realities of children.

7. Acknowledgements

This article is synthesised from the doctoral thesis entitled “Enhancing the Effectiveness of Law Enforcement in Suppressing Human Trafficking: The Production and Distribution of Child Sexual Abuse Materials”, submitted to the Faculty of Social Sciences and Humanities, Mahidol University. The author wishes to express sincere gratitude to thesis advisor Prof Dr Punchada Sirivunnabood for her invaluable guidance throughout the research process. The author is deeply grateful to all key informants whose trust and candour were indispensable to the empirical findings presented herein. This article is dedicated to the author’s parents, whose compassion has been a constant source of strength, to those the author loves and will always watch over, and to all the children in this world who deserve to grow up without losing hope.

8. References

- Açar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology*, 11(1), 98-109. <https://doi.org/10.5281/zenodo.495775>
- ASEAN. (2008). *Anti-Trafficking in Persons Act, B.E. 2551*. Retrieved from <https://asean.org/wp-content/uploads/2016/08/Thailand197.pdf>
- Berger, H., & van de Glind, H. (1999). *Children in prostitution, pornography and illicit activities in Thailand: Magnitude of problems and remedies*. International Labour Organization. Retrieved from https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@asia/@ro-bangkok/documents/publication/wcms_bk_pb_6_en.pdf
- Blackburn, A. G., Taylor, R. W., & Davis, J. E. (2010). Understanding the complexities of human trafficking and child sexual exploitation: The case of Southeast Asia. *Women & Criminal Justice*, 20(1-2), 105-126. <https://doi.org/10.1080/08974451003641099>
- Broadhurst, R. (2019). Child sex abuse images and exploitation materials. *The Human Factor of Cybercrime*. London, UK: Routledge.
- Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). New York, US: Harrow and Heston. https://popcenter.asu.edu/sites/default/files/library/reading/PDFs/scp2_intro.pdf
- CNBC. (2026). *Meta ordered to pay \$375 million after New Mexico child safety trial*. Retrieved from <https://www.cnn.com/2026/03/24/jury-reaches-verdict-in-meta-child-safety-trial-in-new-mexico.html>
- Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag. Retrieved from https://books.google.com/books/about/The_Reasoning_Criminal.html?id=MPmmAgAAQBAJ
- Cullen, O., Ernst, K. Z., Dawes, N., Binford, W., & Dimitropoulos, G. (2020). “Our laws have not caught up with the technology”: Understanding challenges and facilitators in investigating and prosecuting child

- sexual abuse materials in the United States. *Laws*, 9(4), Article 28.
<https://doi.org/10.3390/laws9040028>
- Davy, D. (2014). Understanding the complexities of responding to child sex trafficking in Thailand and Cambodia. *International Journal of Sociology and Social Policy*, 34(11-12), 793-816.
<https://doi.org/10.1108/IJSSP-10-2013-0103>
- ECPAT, INTERPOL, & UNICEF. (2022). *Disrupting harm in Thailand: Evidence on online child sexual exploitation and abuse*. Global Partnership to End Violence against Children. Retrieved from <https://www.unicef.org/innocenti/media/4151/file/DH-Thailand-Report-2022.pdf>
- ECPAT, INTERPOL, & UNICEF. (2023). *Protecting children in Thailand from online sexual exploitation and abuse: The way forward*. Retrieved from https://safeonline.global/wp-content/uploads/2023/12/DH_Thailand_advocacy_brief_FINAL.pdf
- European Country of Origin Information Network. (2003). *Child Protection Act, B.E.* . Retrieved from <https://www.ecoi.net/en/document/1152703.html>
- European Parliament. (2026). *Child sexual abuse online: Support for extending rules until August 2027*. Retrieved from <https://www.europarl.europa.eu/news/en/press-room/20260306IPR37531/child-sexual-abuse-online-support-for-extending-rules-until-august-2027>
- European Union. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*. Retrieved from <http://data.europa.eu/eli/reg/2022/2065/oj>
- Greijer, S., & Doek, J. (2016). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*. ECPAT International and ECPAT Luxembourg.
<https://www.interpol.int/content/download/9373/file/Terminology-guidelines-396922-EN.pdf>
- Hays, K. (2026). *Meta told to pay \$375 million for misleading users over child safety*. BBC. Retrieved from <https://www.bbc.com/news/articles/cql75dn07n2o>
- Internet Watch Foundation (IWF). (2025). *Preventing the upload of child sexual abuse material (CSAM) in end-to-end encrypted environments*. Retrieved from <https://www.iwf.org.uk/media/21rpo2o4/iwf-preventing-the-upload-of-child-sexual-abuse-material-in-end-to-end-encrypted-e2ee-environments-v1.pdf>
- Internet Watch Foundation. (2024). *IWF trustees' report: 31 March 2024*.
<https://www.iwf.org.uk/media/n3ubdxia/iwf-trustees-report-2023-2024.pdf>
- Johnson, A. K. (2014). Protecting children's rights in Asian tourism: Reflecting on progress and the way forward. *The International Journal of Children's Rights*, 22(3), 581-617.
<https://doi.org/10.1163/15718182-02201001>
- Kranrattanasuit, N. (2014). *ASEAN and human trafficking: Case studies of Cambodia, Thailand, and Vietnam* (Vol. 109). Brill Nijhoff. <https://doi.org/10.1163/9789004265189>
- Mangkhalasiri, P. (2024). *Challenges of investigating and prosecuting child sex trafficking and child labour trafficking in Thailand* (Doctoral dissertation). UCL Discovery repository, University College London. Retrieved from <https://discovery.ucl.ac.uk/id/eprint/10206222>
- Mangkhalasiri, P., Khruakham, S., & Phetthong, N. (2025). Data for justice: Potentials and challenges in using state records for human trafficking research in Thailand. *Journal of Thai Justice System*, 18(3), 169–189. Retrieved from <https://so04.tci-thaijo.org/index.php/JTJS/article/view/279137>
- Martin, J., & Alaggia, R. (2013). Sexual abuse images in cyberspace: Expanding the ecology of the child. *Journal of Child Sexual Abuse*, 22(4), 398-415. <https://doi.org/10.1080/10538712.2013.781091>
- Ministry of Digital Economy and Society. (2007). *Computer-Related Crime Act, B.E. 2550*. Retrieved from <https://www.mdes.go.th/law/detail/1907-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007->
- Napier, S., Teunissen, C., & Boxall, H. (2021). How do child sexual abuse live streaming offenders access victims?. *Trends and Issues in Crime and Criminal Justice*, 642, 1-18. <https://doi.org/10.52922/ti78474>
- New Mexico Courts. (2026). *High profile cases*. Retrieved from <https://nmcourts.gov/news/high-profile-cases/>
- Packer, H. L. (1968). *The limits of the criminal sanction*. California, US: Stanford University Press. Retrieved from <https://books.google.com/books?id=gncxJvRGyR0C>

- Piotrowicz, R. W., & Sorrentino, L. (2016). Human trafficking and the emergence of the non-punishment principle. *Human Rights Law Review*, 16(4), 669-699. <https://doi.org/10.1093/hrlr/ngw028>
- Popa, L. (2024). National and international cooperation in investigating crimes of child sexual abuse or sexual exploitation committed by using information technologies. *AGORA International Journal of Juridical Sciences*, 18(1), 102-111. <https://doi.org/10.15837/aijjs.v18i1.6747>
- Prasertsuk, K., Chaiakornwate, A., & Sirirat, J. (2019). *Thailand and non-traditional security: Human trafficking, irregular migration, transnational crime, and cyber crime*. Institute of East Asian Studies, Thammasat University. Retrieved from <https://kpi-lib.com/flippdf/kpiebook62002/kpiebook62002.html#p=1>
- Rafferty, Y. (2007). Children for sale: Child trafficking in Southeast Asia. *Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect*, 16(6), 401-422. <https://doi.org/10.1002/car.1009>
- Republic Act No. 11930, Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Phil. 2022). https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html
- Republic of the Philippines: Philippines Commission on Women. (2022). *Republic Act 11930: Anti-Online Sexual Abuse or Exploitation of Children Act and Anti-Child Sexual Abuse or Exploitation Materials Act*. Retrieved from <https://pcw.gov.ph/republic-act-11930-anti-online-sexual-abuse-or-exploitation-of-children-act-and-anti-child-sexual-abuse-of-exploitation-materials-act/>
- Shapiro, L. R. (2020). Online child sexual abuse material: Prosecuting across jurisdictions. *Journal of Internet Law*, 24(3), 3-8.
- Sharapov, K., Mendel, J., & Schwartz, K. (2024). Expansion, fracturing, and depoliticisation: UK government anti-trafficking funding from 2011 to 2023. *Anti-trafficking Review*, (23), 34-57. <https://doi.org/10.14197/atr.201224233>
- Superior Court of California, County of Los Angeles. (2026). *P.F. v. Meta Platforms: Verdict form - Compensatory damages and claim of punitive conduct*. <https://www.crowell.com/a/web/3poC9PAHEBNpjRbEJNWuoe/verdict-form-compensatory-damages-and-claim-of-punitive-conduct.pdf>
- Thammasiri, K. (2024). Current trends in human trafficking and the effectiveness of law enforcement strategies in combating sex trafficking in Thailand. *Studies in Social Science & Humanities*, 3(7), 12-18. <https://doi.org/10.56397/SSSH.2024.07.02>
- Todres, J. (2010). Taking prevention seriously: Developing a comprehensive response to child trafficking and sexual exploitation. *Vanderbilt Journal of Transnational Law*, 43(1), 1-56. <https://doi.org/10.2139/ssrn.1544301>