

Formulating Social Media Blacklisting as An Additional Criminal Sanction for Online Child Sexual Crimes in Indonesia: A Normative and Comparative Analysis

Muhamad Adystia Sunggara^{1*}, Zico Junius Fernando², Fardana Kusumah³

¹Pertiba University, Indonesia

²Bengkulu University, Indonesia

³Central China Normal University, China

*Correspondence: dr.m.adystiasunggara@gmail.com

Received: July 14, 2025; Accepted: June 26, 2026; Published: June 30, 2026

Abstract

The expansion of social media is transforming the modus operandi of child sexual crimes by enabling offenders to groom, manipulate, exploit, and blackmail children through digital platforms. Indonesia's current criminal justice system remained largely dependent on imprisonment and fines, while the offender's post-conviction access to the same digital environment used to commit the crime was insufficiently regulated. Therefore, this study aimed to examine the possibility of formulating social media blacklisting as an additional criminal sanction for online child sexual crimes in Indonesia. A normative legal study was conducted with statutory, conceptual, and comparative methods to analyse Indonesian criminal law, child protection norms, digital rights, and comparative practices in the United Kingdom, the United States, South Korea, Germany, and Scandinavian jurisdictions. The results showed that social media blacklisting was normatively justified only when it was expressly regulated by statute, imposed by judicial decision, based on individual risk assessment, limited in duration and scope, and subject to proportionality review. This study contributed to penal reform scholarship by proposing a rights-based and risk-based model of digital additional punishment that protected children, prevented digital recidivism, and avoided unconstitutional blanket restrictions on access to information and expression.

Keywords: child protection; social media blacklisting; criminal sanctions; cybercrime; legal innovation

Abstrak

Perkembangan media sosial telah mengubah modus operandi kejahatan seksual terhadap anak dengan memungkinkan pelaku merayu, memanipulasi, mengeksploitasi, dan memeras anak-anak melalui platform digital. Sistem peradilan pidana Indonesia saat ini masih sangat bergantung pada hukuman penjara dan denda, sementara akses pelaku pascaputusan terhadap lingkungan digital yang sama yang digunakan untuk melakukan kejahatan tersebut belum diatur secara memadai. Oleh karena itu, penelitian ini bertujuan untuk mengkaji kemungkinan merumuskan pemblokiran media sosial sebagai sanksi pidana tambahan atas kejahatan seksual terhadap anak secara daring di Indonesia. Penelitian hukum normatif ini dilakukan dengan metode yuridis, konseptual, dan komparatif untuk menganalisis hukum pidana Indonesia, norma perlindungan anak, hak digital, serta praktik komparatif di Inggris, Amerika Serikat, Korea Selatan, Jerman, dan yurisdiksi Skandinavia. Hasil penelitian menunjukkan bahwa pemblokiran media sosial secara normatif dapat dibenarkan hanya jika diatur secara tegas dalam undang-undang,

dijatuhkan melalui putusan pengadilan, didasarkan pada penilaian risiko individu, dibatasi dalam jangka waktu dan cakupannya, serta tunduk pada uji proporsionalitas. Penelitian ini berkontribusi pada kajian reformasi hukum pidana dengan mengusulkan model hukuman tambahan digital berbasis hak dan risiko yang melindungi anak-anak, mencegah residivisme digital, serta menghindari pembatasan menyeluruh yang bertentangan dengan konstitusi terhadap akses informasi dan kebebasan berekspresi.

Kata kunci: daftar hitam media sosial; sanksi pidana; inovasi hukum; kejahatan siber; perlindungan anak

Introduction

The rapid advancement of information and communication technology is reshaping human interaction and the methods of socialisation, especially among children and adolescents.¹ Social media platforms, such as Facebook, Instagram, TikTok, and WhatsApp, have become integral to the daily lives of young people, providing an always-connected digital environment.²

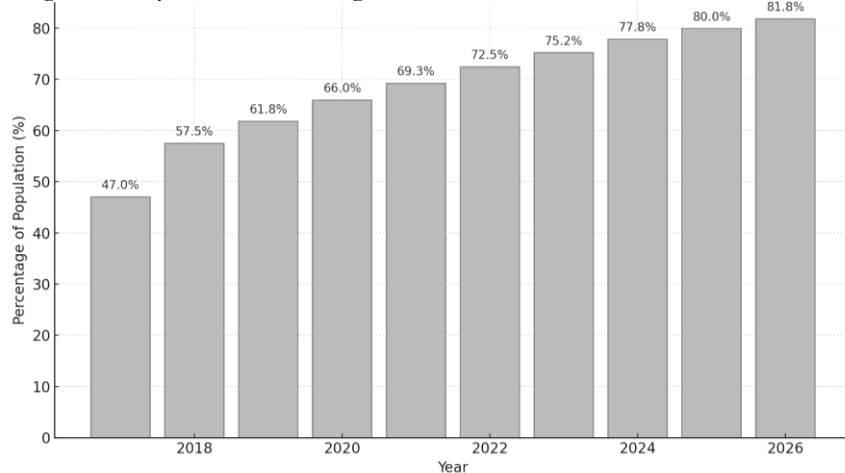


Figure 1. Social Media Users in Indonesia (2017–2026)

Source: Authors' visualisation based on Data Reportal and Statista

The illustration in Figure 1 shows that social media usage in Indonesia has grown rapidly and consistently, rising from 47.03% of the population in 2017 to a projected 81.82% in 2026. Young children's and adolescents' social media use increased beyond a demographic phenomenon and represented a criminologically relevant development. Expanding social media use produced a wider digital environment where children and adolescents interacted, communicated, and faced exposure to online grooming, sextortion, and other forms of technology-facilitated

¹ Yesya Vatria Barasa et al., "Pengaruh Human Relations Terhadap Interaksi & Perilaku Remaja Di Media Sosial," *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 1, no. 6 (December 2024): 166–73, <https://doi.org/10.62383/KONSENSUS.V1I6.480>.

² Gayatri Sunkad, "The Impact of Social Media on Society," *International Journal of Social Health* 2, no. 10 (November 2023): 785–91, <https://doi.org/10.58860/IJSH.V2I10.121>.

sexual exploitation. Therefore, Figure 1 provides the empirical background for the study's normative argument that Indonesia's sentencing system must be capable of responding to crimes committed through social media platforms.³

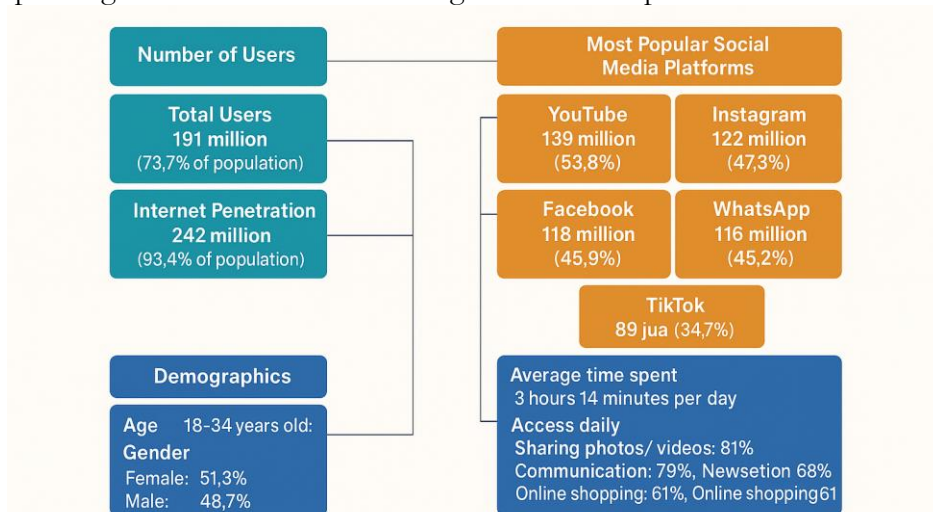


Figure 2. Indonesia's Digital Society: Key Insights into Social Media Usage in 2024

Source: Authors' visualisation based on Databoks/Katadata

The data in Figure 2 shows that social media usage in Indonesia in 2024 reflects extensive access and intense daily engagement. The total number of social media users reached 191 million, representing 73.7% of the population, while active users numbered 167 million, representing 64.3%. The country's internet penetration was remarkably high, with 242 million users, or 93.4% connected online. In terms of platform popularity, YouTube remains the most used platform with 139 million users (53.8%), followed by Instagram, Facebook, WhatsApp, and TikTok with 122 million (47.3%), 118 million (45.9%), 116 million (45.2%), and 89 million users (34.7%), respectively. The 18–34 age group dominates social media usage, accounting for 54.1%, while the gender distribution is relatively balanced, with 51.3% female and 48.7% male users. Indonesians spend an average of 3 hours and 14 minutes per day on social media, and 81% of users access social media daily. The most common activities include sharing photos/videos, communication, accessing news/information, entertainment, and online shopping, with percentages of 81%, 79%, 73%, 68%, and 61%, respectively.⁴ Remarkably, over 14% of these users were aged between 13 and 17 years. This figure shows the deep penetration of digital culture among children and adolescents, making social media both a tool for communication and a central aspect of social identity and interaction.

³ Agnes Yonatan, "Menilik Pengguna Media Sosial Indonesia 2017-2026," data.goodstats.id, 2023.

⁴ Andreas Daniel Panggabean, "Ini Data Statistik Penggunaan Media Sosial Masyarakat Indonesia Tahun 2024," RRI.co.id, 2024.

The relevance of these figures is sociological and penal. The increasing intensity of children's interaction with social media expands the opportunity structure for offenders who use digital platforms as instruments of grooming, coercion, sextortion, and distribution of child sexual abuse material. Therefore, the growth of social media use must be read as part of a broader transformation in the ecology of crime. Criminal law can no longer respond only to the physical act of abuse or the final harmful consequence. Addressing the digital environment that supports the offence also remains necessary. This is the starting point for reconsidering whether conventional sanctions are sufficient, or whether a more targeted form of additional punishment is required to prevent convicted offenders from re-entering the same online spaces used to harm children.

The rise of social media has introduced complex challenges despite the positive contributions of digital connectivity, particularly concerning the safety and rights of children.⁵ The digital realm, often perceived as neutral or even empowering, has evolved into a fertile ground for criminal acts, including sexual exploitation, online grooming, child pornography, and trafficking.⁶ According to data from the Indonesian Child Protection Commission (KPAI) as of June 2024, there were 1,193 recorded cases of child protection violations. A total of 893 cases included violations of children's rights fulfilment, while 300 cases fell under the category of special child protection violations. In the area of rights fulfilment, the highest number of cases included children who were victims of problematic caregiving, totalling 486 cases. This was followed by children affected by policies in educational settings, with 84 cases. For special protection violations, the highest number of cases included child victims of sexual violence, with 116 cases, followed by physical and psychological abuse, totalling 101 cases. Furthermore, KPAI reported 46 cases of children committing self-harm, including suicide attempts, with 22 of those incidents occurring within educational institutions or outside school premises while the children were still wearing school uniforms.⁷

Online child sexual exploitation differs significantly from conventional crimes.⁸ Offenders use the anonymity and wide reach of social media to manipulate, lure, and threaten victims who lack adequate digital literacy or self-

⁵ Ben Wagner, Matthias C. Kettmann, and Kilian Vieth, *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*, *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations* (Edward Elgar Publishing, 2019), <https://doi.org/10.4337/9781785367724>.

⁶ Yiyin Xu, "Digital Dangers: How Technology Has Transformed Child Sexual Exploitation," *Advances in Education, Humanities and Social Science Research* 13, no. 1 (March 2025): 99–99, <https://doi.org/10.56028/AEHSSR.13.1.99.2025>.

⁷ Anita Permata Dewi, "KPAI: HAN 2024 Momentum Lindungi Anak Di Ranah Daring," ANTARA News, 2024.

⁸ Marie Henshaw, James R P Ogloff, and Jonathan A. Clough, "Demographic, Mental Health, and Offending Characteristics of Online Child Exploitation Material Offenders: A Comparison with Contact-only and Dual Sexual Offenders," *Behavioral Sciences & the Law* 36, no. 2 (March 16, 2018): 198–215, <https://doi.org/10.1002/bsl.2337>.

protection awareness.⁹ A prominent case in 2023 included a 34-year-old man (initials MA), arrested by the Jakarta Metropolitan Police for sexually exploiting underage girls through TikTok and Instagram. By impersonating an adolescent, the perpetrator built trust with the victims online, engaged in emotional manipulation, and eventually used coercion to receive explicit content.¹⁰ The perpetrator then blackmailed the victims under threat of public exposure. Law enforcement showed that at least 17 girls from various regions were victimised in just six months, exposing the scale and velocity with which digital crimes can unfold. These cases show that the digital space can become perilous without strict regulation, especially concerning the protection of minors. Unfortunately, Indonesia's current criminal law system has yet to fully adapt to the realities of digital-based crimes.¹¹ Although the Law on Electronic Information and Transactions and the Child Protection Law (Law No. 35 of 2014) provide general provisions to combat cyber offences and protect minors, there is no specific mechanism that restricts or bans digital access, especially access to social media, as part of criminal sentencing.¹²

In this article, social media blacklisting refers to a court-ordered additional criminal sanction. Court orders temporarily prohibit convicted offenders from accessing, creating, operating, or using specified social media accounts or digital communication platforms directly connected to the commission, preparation, concealment, or repetition of online child sexual crimes. The concept should not be equated with a general internet ban or a permanent exclusion from digital life. It is a targeted, risk-based, and judicially supervised restriction imposed only when there is a clear nexus between the offender's digital conduct and the criminal offence. The scope may include prohibitions on anonymous accounts, on contact with minors via digital platforms, on the use of specific applications, or on creating new accounts without notifying supervising authorities. This type of sanction must be time-bound, reviewable, and supported by procedural safeguards to prevent excessive interference with freedom of expression, access to information, employment, education, and social reintegration.¹³

⁹ Željko Đ. Bjelajac and Aleksandar M. Filipović, "Flexibility of Digital Media for Manipulative Activities of Sexual Predators," *KULTURA POLISA* 18, no. 44 (March 2021): 51–67, <https://doi.org/10.51738/KPOLISA2021.18.1R.2.01>.

¹⁰ Malin Joleby et al., "Offender Strategies for Engaging Children in Online Sexual Activity," *Child Abuse & Neglect* 120 (October 2021): 1–5, <https://doi.org/10.1016/J.CHIABU.2021.105214>.

¹¹ Ida Musofiana, Aji Sudarmaji, and Ira Alia Maerani, "Aspects of Legal Protection for Children from Cybercrime," *Jurnal Pembaharuan Hukum* 7, no. 3 (December 2020): 201–10, <https://doi.org/10.26532/JPH.V7I3.12820>.

¹² Ranto Daniel Panjaitan and Diki Zukriadi, "Pertanggung Jawaban Hukum Terhadap Anak Sebagai Korban Cyberbullying Pada Media Sosial," *SCIENTIA JOURNAL: Jurnal Ilmiah Mahasiswa* 6, no. 3 (February 2024): 1–10, <https://doi.org/10.33884/SCIENTIAJOURNAL.V6I3.8277>.

¹³ Sarah Kingston and Terry Thomas, "The Sexual Risk Order and the Sexual Harm Prevention Order," *Probation Journal* 65, no. 1 (March 7, 2018): 77–88, <https://doi.org/10.1177/0264550517748359>.

Considering the rise in digital sexual crimes against minors in Indonesia, implementing social media blacklisting could be a significant and progressive step forward.¹⁴ The Financial Transaction Reports and Analysis Centre (PPATK) and the Indonesian National Police have observed a sharp rise in suspicious financial transactions associated with child exploitation through digital platforms, including live-streamed child pornography and financial extortion.¹⁵ These patterns suggest that digital child sexual exploitation is not only prevalent but also economically organised, involving cross-border networks and criminal syndicates.¹⁶ Normatively, the rationale for introducing social media blacklisting as a form of criminal sanction is consistent with the principles of proportionality and rehabilitation in criminal justice. Criminal punishment is aimed not only at retribution but also at protecting society and preventing reoffending.¹⁷ Restricting digital access to offenders is a rational penalty, especially when the crime was committed through social media. It directly targets the tools and environment through which the offence occurred and aims to reduce the tendency of digital recidivism, namely, the potential for reoffending through new digital identities or accounts.¹⁸

The implementation of these sanctions does raise legal and ethical questions. Critics have raised concerns about enforceability, privacy rights, and the risk of disproportionately infringing on offenders' freedom of expression or reintegration into society. However, comparative legal analysis suggests that many jurisdictions have recognised digital restriction orders as a legitimate component of sentencing, provided that the restrictions are proportionate, time-bound, and specifically designed to mitigate the risk posed by the offender.¹⁹ In Indonesia, the primary challenge to introducing social media blacklisting is the absence of a supporting legal framework. The new Indonesian Penal Code (*KUHP Nasional*), enacted through Law No. 1 of 2023, does not explicitly address digital restrictions or ancillary sanctions related to internet or social media use. Similarly, the Draft Criminal Procedure Code (*Rancangan KUHAP*) does not offer procedural mechanisms for enforcing digital

¹⁴ Sandi Aprianto and Widya Timur, "Juridical Review of the Role of Society Against Sexual Crimes of Minors Through Gadgets Based on Law Number 19 of 2016 Concerning Information and Electronic Transactions," *JURNAL HUKUM SEHASSEN* 9, no. 1 (April 2023): 41-50-41 – 50, <https://doi.org/10.37676/JHS.V9I1.3893>.

¹⁵ Karima Naila Putri, Kiki Kristanto, and Yurika F.Dewi, "Criminal Liability for Indonesians Who Use Digital Wallets to Commit Child Sexual Exploitation," *Journal of Law, Politic and Humanities* 5, no. 3 (January 2025): 2043–52, <https://doi.org/10.38035/JLPH.V5I3.1434>.

¹⁶ Roderic Broadhurst, *Child Sex Abuse Images and Exploitation Materials, The Human Factor of Cybercrime* (Routledge, 2019), <https://doi.org/10.4324/9780429460593-14>.

¹⁷ Lauren Shaw, "A Cross Comparison of Temporary Work Release Programs as an Alternative to Incarceration Within Canada and Ukraine," *Crossing Borders: Student Reflections on Global Social Issues* 4, no. 1 (November 2022): 1–10, <https://doi.org/10.31542/CB.V4I1.2478>.

¹⁸ Bianca C. Reisdorf and Yvonne Jewkes, "(B)Locked Sites: Cases of Internet Use in Three British Prisons," *Information Communication and Society* 19, no. 6 (June 2016): 771–86.

¹⁹ Michiel van der Wolf, "Legal Control on Social Control of Sex Offenders in the Community: A European Comparative and Human Rights Perspective," *Erasmus Law Review* 9, no. 2 (December 2016): 39–54, <https://doi.org/10.5553/ELR.000074>.

sanctions or monitoring offenders' online activities. This legal vacuum makes it difficult for law enforcement and the judiciary to impose effective post-conviction digital controls, even in cases involving vulnerable child victims. To address this gap, legislative and judicial interventions are needed to develop new normative instruments that are consistent with contemporary digital realities. The legal principle of *ius curiae novit* allows judges to interpret and apply the law in light of society's needs, especially where there are legal ambiguities or gaps.²⁰ In the landmark U.S. Supreme Court case of *Packingham v. North Carolina* (2017), the Court acknowledged the importance of proportionality in regulating offenders' access to social media, holding that child protection constituted a compelling state interest.²¹ Although the Court invalidated a blanket ban on social media access as overbroad, it affirmed that digital restrictions were permissible when narrowly tailored to prevent harm.

In the Indonesian context, a social media blacklisting policy required a statutory basis and a collaborative framework between law enforcement, digital platform providers, the Ministry of Communication and Information, and child protection institutions. Effective enforcement depended on digital forensics, user tracking systems, and post-release monitoring technologies. For instance, countries such as South Korea use electronic bracelets and mandatory residence declarations for sex offenders, along with restrictions on internet access as part of broader rehabilitation and surveillance strategies.

The growing need for child protection in the digital sphere was underscored by the increasing number of cross-border child sexual exploitation cases.²² In 2023, the international child pornography ring "*Bastara Net*" was uncovered by Interpol in collaboration with Southeast Asian authorities.²³ Several Indonesian perpetrators faced arrest for exploiting children online through anonymous chat platforms and encrypted social media applications. Victims included young girls with a minimum age of nine years, from Indonesia's eastern provinces. The perpetrators initiated contact via mainstream platforms, such as Facebook and Telegram, before moving to more private, less traceable ones.²⁴ This case showed the real and present danger

²⁰ Loso Judijanto, Nuryati Solapari, and Imman Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *The Easta Journal Law and Human Rights* 3, no. 01 (October 2024): 20–29, <https://doi.org/10.58812/ESLHR.V3I01.351>.

²¹ Alejandro Herrán Aguirre, "Derecho a La Libertad de Expresión y Acceso a Las Redes Sociales: El Caso Packingham Con Carolina Del Norte," *Revista Chilena de Derecho y Tecnología* 7, no. 2 (December 2018): 163–86, <https://doi.org/10.5354/0719-2584.2018.49020>.

²² Sabine K. Witting, "Transnational by Default: Online Child Sexual Abuse Respects No Borders," *The International Journal of Children's Rights* 29, no. 3 (August 2021): 731–64, <https://doi.org/10.1163/15718182-29030010>.

²³ Nabilah Hani Ahmad Zubaidi, "Monitoring Internet Child Pornography (ICP) in Malaysia," *Pertanika Journal of Social Sciences and Humanities* 29 (2021): 185–203, <https://doi.org/10.47836/PJSSH.29.S2.13>.

²⁴ Luh Putu Vera Astri Pujayanti et al., "Legal Review of Child Grooming as A Crime of Sexual Violence in Indonesia," *Jurnal Hukum Dan HAM Wara Sains* 2, no. 03 (March 2023): 188–96, <https://doi.org/10.58812/JHHWS.V2I03.252>.

of unregulated digital spaces when exploited by predators. These incidents also showed the role of offenders and the systemic weaknesses in national laws and enforcement mechanisms. Legal tools restricting digital access after conviction remained necessary to reduce repeat offences and continued harm to children. Absence of legal restrictions increased the risk of repeat offences and prolonged harm to children. Therefore, the state's responsibility to safeguard vulnerable groups must evolve in parallel with technological changes and developing threats.

The adoption of social media blacklisting as a criminal sanction would necessitate a redefinition of criminal liability in the digital age. Traditional sanctions, such as imprisonment or fines, target the offender's physical liberty and financial capacity. However, digital sanctions must extend to the offender's virtual identity, communication platforms, and digital interactions. Some European countries, such as the United Kingdom (via Digital Restriction Orders) and Germany (through administrative Internet bans), have already begun to implement sanctions that restrict digital access, reflecting an expanded conception of punitive and preventive justice in response to digital crimes. For Indonesia to move forward, it must prioritise the development of legal instruments that authorise digital-based sanctions, supported by clear enforcement procedures and technology-driven monitoring systems. This initiative would not only fulfil the constitutional mandate of child protection as guaranteed under Article 28B(2) of the 1945 Constitution but also comply with international obligations under the United Nations Convention on the Rights of the Child (CRC), particularly the 2021 General Comment No. 25 on children's rights in the digital environment.²⁵ By acknowledging the digital environment as both a risk and an opportunity, Indonesia can adopt a more nuanced, responsive, and rights-oriented method for child protection. The incorporation of social media blacklisting into the criminal justice system should be carefully crafted to balance rehabilitation, deterrence, and the paramount principle of the best interest of the child.

Existing legal scholarship in Indonesia has generally discussed online child protection through the lens of cybercrime regulation, the Electronic Information and Transactions Law, child protection statutes, or victim-oriented criminal justice. However, limited attention has been given to the doctrinal construction of digital access restriction as an additional criminal sanction within Indonesia's sentencing system. This study fills that gap by formulating social media blacklisting as a technological policy and also a penal instrument that must satisfy the requirements of legality, proportionality, judicial authorisation, and post-sentence supervision. The novelty of this study is in its attempt to connect child protection in the digital environment with the structure of additional punishment under Indonesian criminal law, while drawing comparative lessons from jurisdictions that have

²⁵ Sonia Livingstone et al., "The UN Committee on the Rights of the Child's General Comment on the Digital Environment," *AoIR Selected Papers of Internet Research*, March 2022, 1–12, <https://doi.org/10.5210/SPiR.V2022I0.12960>.

developed risk-based digital restrictions for sexual offenders. Therefore, this study offers a normative model that is both protective of children and sensitive to constitutional limits on state interference with digital rights.

Methods

A normative legal study method was adopted, focusing on examining legal norms as the principal object of analysis.²⁶ The method remained appropriate because the main issue addressed in the study, social media blacklisting as a criminal sanction for protecting children in the digital era, lacked explicit regulation under current Indonesian criminal law. Normative legal study allowed the analyst to critically analyse existing legal rules, identify normative gaps, and formulate legal propositions that were responsive to developing social threats, such as online child sexual exploitation.²⁷ This study employed three core methods: statutory, conceptual, and comparative law. *First*, the statutory method included an in-depth review of relevant Indonesian laws, including Law No. 35 of 2014 on Child Protection, Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law), and Law No. 1 of 2023 on the Criminal Code (KUHP). It also examined the Draft Criminal Procedure Code (RKUHAP) to assess the potential integration of digital sanctions, such as bans on social media access, into Indonesia's sentencing and post-conviction supervision systems. Furthermore, the UN Convention on the Rights of the Child (CRC) and General Comment No. 25 (2021) were referred to as normative benchmarks for child protection in the digital environment.

Second, the conceptual approach was used to explore and elaborate on the legal concept of social media blacklisting. This method provided a theoretical foundation by reviewing literature on criminal sanctions, digital identity regulation, and child-centred justice. The notion of sanctioning digital access represented a shift in penal theory from traditional custodial punishment to a more targeted restriction that directly addressed the means by which online offences were committed. It also engaged with legal principles, such as proportionality, necessity, and rehabilitation, in shaping new forms of punishment in the context of digital crimes. *Third*, the comparative law method was adopted to strengthen the normative analysis by observing how other jurisdictions have responded to similar challenges. In the United States, various state-level laws prohibited child sex offenders from using or creating social media accounts, particularly when the platforms were used to groom victims. However, these laws faced constitutional scrutiny, including in *Packingham v. North Carolina* (2017), which highlighted the need to balance child safety with freedom of expression. In the United Kingdom, courts were empowered to impose Sexual Harm Prevention Orders (SHPOs) that

²⁶ Yagie Sagita Putra et al., "EIT Law at the Crossroads: Exploring Legal Dilemmas, Freedom of Expression, and Human Rights," *Pakistan Journal of Criminology* 16, no. 3 (July 2024): 1315–32, <https://doi.org/10.62271/PJC.16.3.1315.1332>.

²⁷ Zico Junius Fernando et al., "The Freedom of Expression in Indonesia," *Cogent Social Sciences* 8, no. 1 (July 2022): 1–11, <https://doi.org/10.1080/23311886.2022.2103944>.

included restrictions on internet and device use. In South Korea, convicted sex offenders were subject to strict monitoring and could face limitations on residence, employment, and digital activity. Germany adopted administrative sanctions, such as Internetsperre, especially in cases including extremist content and child pornography, as part of broader preventive mechanisms. This study used both descriptive and prescriptive methods²⁸ to systematically present the growing phenomenon of online child sexual exploitation and analyse the current limitations in Indonesia's legal system in addressing the crimes.

The study identified gaps in substantive criminal law and sentencing frameworks that failed to regulate offenders' access to digital platforms after conviction. Furthermore, a normative construction of social media blacklisting was proposed as a criminal sanction. This included exploring the theoretical justification, legal feasibility, and potential integration into Indonesian criminal legislation and policy. Primary (statutes, judicial decisions, and international instruments), secondary (textbooks, academic journal articles, legal commentaries, and official reports), and tertiary sources (legal dictionaries, encyclopedias, and indexing systems) were used in this study.²⁹ The materials were analysed using content analysis, a method that included identifying key legal principles, interpreting normative content, and assessing the relevance to contemporary social phenomena.³⁰ Through this method, the study aimed to provide a structured legal framework that supported the development of digital sanctions designed to protect children in the online environment. By combining these methods and analytical tools, this study contributed to the academic discourse on digital penal reform and provided a normative model for future legislation. It also advocated for a more adaptive and forward-looking criminal justice system that was consistent with technological realities and prioritised the rights and safety of children as a vulnerable group in the digital age.³¹

²⁸ Zico Junius Fernando et al, "Cyber Victimology and Legal Gaps in Southeast Asia," *International Law Discourse in Southeast Asia* 4, no. 1 (June 2025): 1–39, <https://doi.org/10.15294/ILDISEA.V4I1.20147>.

²⁹ Mahrus Ali et al., "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims," *Substantive Justice International Journal of Law* 8, no. 1 (May 2025): 1–12, <https://doi.org/10.56087/SUBSTANTIVEJUSTICE.V8I1.306>.

³⁰ Emi Puasa Handayani, Zainal Arifin, and Zico Junius Fernando, "Criminal Penalties in Cyberspace: Between the Development of Digital Democracy and Authoritarianism," *Indonesian Journal of Criminal Law Studies* 10, no. 1 (May 2025): 45–82, <https://doi.org/10.15294/IJCLS.V10I1.19652>.

³¹ Zainal Arifin, Zico Junius Fernando, and Emi Puasa Handayani, "Implikasi Hukum Perubahan Kedua Undang-Undang Informasi Dan Transaksi Elektronik: Menyeimbangkan Kebebasan Berpendapat Dan Partisipasi Publik Dalam Demokrasi Digital: Legal Implications of The Second Amendment to The Electronic Information and Transactions Law: Balancing Freedom of Expression and Public Participation in Digital Democracy," *LITIGASI* 26, no. 1 (April 2025): 192–227, <https://doi.org/10.23969/LITIGASI.V26I1.21555>.

Results and Discussions

The Urgency of Sentencing Reform in Responding to Digital Sexual Crimes Against Children

The rapid advancement of digital technology has significantly transformed human life in various aspects, particularly in how individuals interact and communicate. Social media has become a powerful medium for self-expression and socialisation, particularly among children and adolescents. Platforms such as TikTok, Instagram, and Facebook have become inseparable from children's daily routines, providing opportunities for connection and access to information.³² However, this digital technology has evolved into a breeding ground for new forms of criminal behaviour, particularly online sexual crimes targeting children, who represent a highly vulnerable group in cyberspace.³³

Digital sexual crimes against children, which include grooming, online child sexual exploitation, sextortion, and the distribution of child sexual abuse material, have increased both in scale and sophistication.³⁴ According to the KPAI, more than 40 per cent of reported sexual violence cases against children included the use of social media as a primary tool. This trend showed a clear shift in the modus operandi of offenders, moving from traditional, physical proximity to manipulative engagement in virtual environments, often hidden from parents, schools, and law enforcement agencies.³⁵

Perpetrators often use fake profiles and assumed identities to interact with victims, gradually building emotional connections that culminate in sexual exploitation.³⁶ Some offenders recorded or requested explicit content, which was later used for blackmail purposes in the form of sextortion. Digital patterns of abuse occurred within private online spaces, reducing detection and prevention through conventional mechanisms.³⁷ The invisibility of the crimes, combined with the

³² Nyiramana Mukamurera P., "The Impact of Social Media on Mental Health," *Research Invention Journal Of Research In Medical Sciences* 4, no. 1 (March 2025): 11–15, <https://doi.org/10.59298/RIJRMS/2025/411115>.

³³ Andrejs Vilks, "Cybercrime and Sexual Exploitation of Children in E-Environment in the Context of Strengthening Urban and Rural Security," *SHS Web of Conferences* 68 (2019): 1–11, <https://doi.org/10.1051/SHSCONF/20196801010>.

³⁴ Kyung-Shick Choi and Hannarae Lee, "The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response," *Journal of Child Sexual Abuse*, n.d., 1–20, <https://doi.org/10.1080/10538712.2023.2214540>.

³⁵ Juliane A. Kloess et al., "A Qualitative Analysis of Offenders' Modus Operandi in Sexually Exploitative Interactions With Children Online," *Sexual Abuse* 29, no. 6 (September 10, 2017): 563–91, <https://doi.org/10.1177/1079063215612442>.

³⁶ Arezou Behfar, Ankit Shrestha, and Mahdi Nasrullah Al-Ameen, "A First Look into Fake Profiles on Social Media through the Lens of Victim's Experiences," in *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing* (New York, NY, USA: ACM, 2024), 444–50, <https://doi.org/10.1145/3678884.3681889>.

³⁷ Molly Dragiewicz et al., "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms," *Feminist Media Studies* 18, no. 4 (July 2018): 609–25, <https://doi.org/10.1080/14680777.2018.1447341>.

psychological manipulation, rendered children extremely vulnerable and further complicated legal intervention. From a criminal justice perspective, the increasing prevalence of digital sexual crimes poses significant challenges. Despite incorporating elements of cybercrime and child protection in the ITE Law and the Child Protection Law (Law No. 35 of 2014), Indonesia's current criminal legal framework remains rooted in traditional notions of crime and punishment.³⁸ Sentences tended to depend on imprisonment or monetary fines without accounting for the digital infrastructure that enabled the crimes in the first place. Therefore, unrestricted access for offenders to digital tools and social platforms remained an underlying source of harm.

The inadequacy of conventional punishment was in its failure to disrupt the offender's digital opportunity structure. Imprisonment temporarily incapacitated the offender in the physical world, but it did not necessarily eliminate the criminogenic relationship between the offender, the digital platform, and potential child victims after release. Fines addressed the economic aspect of punishment but did not respond to the technological means through which grooming, coercion, and exploitation were conducted. In online child sexual crimes, the danger did not end when the offender leaves prison. It could reappear when offenders regain access to anonymous accounts, encrypted messaging applications, or platforms populated by children. Therefore, sentencing reform was necessary to ensure that punishment addressed the offender's past act and the future risk created by unrestricted digital access. This gap was particularly evident in the absence of sentencing mechanisms that restricted offenders' access to digital spaces following conviction. In many cases, individuals who have served prison terms regain unrestricted access to the same digital platforms used to victimise children, thereby posing a continued risk to society. The lack of digitally based supplementary sanctions reflected a systemic failure to implement crime-specific sentencing policies consistent with the nature of cyber-enabled offences.

Within the field of penal theory, sentencing must be evaluated based on its purposes and effectiveness in addressing specific criminal conduct. Three dominant theories of punishment, retributive, utilitarian, and rehabilitative, offer different justifications for imposing sanctions.³⁹ The retributive theory focused on punishment as moral retribution for wrongdoing. However, utilitarian theory viewed punishment as a tool for deterrence, both general (to society) and specific (to the offender). The rehabilitative theory promotes reforming the offender to prevent future crimes. When viewed through utilitarian and rehabilitative lenses, traditional custodial sanctions were insufficient in curbing digital sexual crimes. Offenders familiar with online platforms could easily reoffend unless access to the digital realm was restricted. In this context, sentencing must extend beyond physical deprivation

³⁸ Wieke Dewi Suryandari, "Efforts to Reform Law Enforcement in Tackling Cybercrime," *International Journal of Law Social Sciences and Management* 1, no. 2 (April 2024), <https://doi.org/10.69726/IJLSSM.V1I2.27>.

³⁹ Sue Rex, "Punishment as Communication," in *Alternatives to Prison* (Willan, 2013), 131–52, <https://doi.org/10.4324/9781843925743-12>.

and target the offender's ability to manipulate online tools. Digital-based sanctions, including social media blacklisting, represented relevant and proportionate responses for preventing recidivism and limiting potential harm.

In tandem with penal theory, legal protection for vulnerable groups underscored the need for targeted legal instruments to protect children, who were structurally disadvantaged in digital interactions.⁴⁰ Limited digital literacy, dependence on adult supervision, and psychological susceptibility placed children in a weak position vis-à-vis online predators.⁴¹ Therefore, sentencing schemes must be recalibrated to recognise this power imbalance and provide designed protection, particularly when the crime includes abuse of digital environments. Several jurisdictions have undertaken significant reforms to address this problem. In the United Kingdom, the use of SHPOs enabled courts to impose behavioural restrictions on sex offenders, including bans on internet use or accessing specific digital platforms.⁴² These orders were grounded in risk-based assessments and are implemented in addition to prison sentences. Restrictions prohibited the offender from owning more than one internet-enabled device, using anonymous online accounts, or participating in certain digital communities.

In the United States, many states enacted laws restricting the use of social media by convicted sex offenders. However, *Packingham v. North Carolina* (2017) invalidated a blanket ban on social media use because the prohibition violated the First Amendment.⁴³ The Court left open the possibility for narrowly designed restrictions that were justified by legitimate governmental interests, such as child protection. Digital restrictions remained permissible under proportionate and offence-specific conditions. Proportionality and offence-specific limitations remained necessary.

In South Korea, a stricter regime existed, including the public registry of child sex offenders. Offender personal information remained publicly accessible, accompanied by intensive surveillance, including potential digital monitoring.⁴⁴ These measures were accompanied by mandatory declarations of residence and employment restrictions. Legitimate privacy concerns accompanied the policies, yet

⁴⁰ Musofiana, Sudarmaji, and Maerani, "Aspects of Legal Protection for Children from Cybercrime."

⁴¹ Ellen Johanna Helsper and David Smahel, "Excessive Internet Use by Young Europeans: Psychological Vulnerability and Digital Literacy?," *Information, Communication & Society* 23, no. 9 (July 2020): 1255–73, <https://doi.org/10.1080/1369118X.2018.1563203>.

⁴² Graeme Horsman, "Reviewing the Devices of Those Subject to Sexual Harm Prevention Orders (SHPOs): IOS Opportunities, Limitations and Strategies," *Australian Journal of Forensic Sciences* 57, no. 1 (January 2025): 16–38, <https://doi.org/10.1080/00450618.2023.2252472>.

⁴³ Karen J Terry, "Sex Offender Laws in the United States: Smart Policy or Disproportionate Sanctions?," *International Journal of Comparative and Applied Criminal Justice* 39, no. 2 (April 2015): 113–27, <https://doi.org/10.1080/01924036.2014.973048>.

⁴⁴ Jaekyung Ahn, Sung Yon Han, and Yimoon Choi, "Reassessing Residency Restrictions: Analyzing Crime Proximity and Patterns for Sex Offenders in South Korea," *International Journal of Offender Therapy and Comparative Criminology* 69, no. 10–11 (August 2025): 1524–43, <https://doi.org/10.1177/0306624X251317575>.

available evidence indicated that the policies were effective in deterring repeat offences and enhancing public safety, particularly in urban areas with high internet penetration. From the perspectives of social defence theory and victimology, criminal punishment must serve as retribution and as a means of defending society and preventing victimisation.⁴⁵ Crimes committed in virtual spaces require sentencing measures that restrict offenders' reentry into digital environments previously used to cause harm.⁴⁶ In cases of digital sexual crimes, this implies restricting access to social media platforms and communication technologies.

Indonesia's current legal framework has yet to integrate the digital-based restrictions. The new Criminal Code (KUHP 2023), although modernised in various aspects, did not explicitly recognise digital access bans or social media blacklisting as valid sentencing options. Similarly, the Draft Criminal Procedure Code (RKUHAP) failed to provide procedural mechanisms for issuing and enforcing the sanctions. The judiciary lacked both the normative and procedural tools needed to protect children from digital recidivism by previously convicted offenders. However, contemporary criminal law recognised a broader spectrum of punishments beyond imprisonment or fines. In several jurisdictions, conditional sentencing, digital surveillance, and behavioural injunctions were standard tools in the penal arsenal. These modern sentencing models aimed to address the specific nature of crimes and were adaptable to the offender's behaviour. In Indonesia, the law could be reformed to enable courts to impose digital access bans as ancillary penalties, especially in cases where social media served as a conduit for sexual abuse. However, legal reform was not limited to statutory amendments. Effective implementation of digital-based sanctions requires a multidisciplinary framework including law enforcement, the judiciary, social services, internet service providers, and social media companies.⁴⁷ For instance, executing a court order to block access to a platform would require collaboration with global digital providers, such as Meta (Facebook, Instagram) or ByteDance (TikTok). The result showed the need for a cross-sectoral legal method consistent with technological capacities and regulatory mandates.⁴⁸ Criminological studies showed that many online child sex offenders were not conventional criminals but individuals with high digital proficiency and psychological tendencies toward

⁴⁵ Woo Sik Chung, "An Empirical Validation of a Theory of Punishment," *International Journal of Comparative and Applied Criminal Justice* 18, no. 1–2 (January 1994): 221–48, <https://doi.org/10.1080/01924036.1994.9689039>.

⁴⁶ Kamil Mamak, "Cyber Banishment: An Old Sanction for Virtual Spaces," *Criminal Justice Studies* 36, no. 2 (April 2023): 133–45, <https://doi.org/10.1080/1478601X.2023.2188449>.

⁴⁷ Stanislaw Tosza, "Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors," *Computer Law & Security Review* 43 (November 2021): 1–5, <https://doi.org/10.1016/J.CLSR.2021.105614>.

⁴⁸ Ni Putu Ega and Maha Wiryanthi, "Copyright Infringement in Online Media: Corporate Legal Liability," *Al-Adalah: Jurnal Hukum Dan Politik Islam* 10, no. 1 (January 2025): 151–67, <https://doi.org/10.30863/AJMPL.V10I1.7681>.

manipulation and abuse.⁴⁹ Without addressing digital behaviour, traditional incarceration often failed to rehabilitate or deter these offenders. A sentencing system that targets online behaviour and digital identities tends to be more effective in reducing repeat offences and mitigating harm. Modern criminal justice systems were increasingly called to answer three key questions, namely (1) whom is the law protecting? (2) what type of crime is being addressed? and (3) what form of punishment is most effective? In the context of digital sexual crimes against children, the law must protect victims, address crimes committed through technological means, and impose penalties that disrupt offenders' access to digital environments that enable abuse.⁵⁰

The growing urgency of sentencing reform was further supported by international guidance. UNICEF's report on *Child Protection in the Digital Environment* recommended that states develop sanctions targeting digital behavior and technology access. Similarly, the UNODC's *Guidelines on the Protection of Child Victims in Cyberspace* call for national legislation that was responsive to cyber-enabled crimes and explicitly considered digital restrictions as part of sentencing policy.⁵¹ Viewed through these legal and theoretical frameworks, sentencing for digital sexual crimes against children must evolve to meet the unique characteristics of the offences and the realities of the digital era. Exclusive reliance on traditional penalties without addressing continued offender access to platforms used for abuse failed to protect children effectively and increased the risk of continued harm.

Digital Sanctions in Comparative Legal Systems and the Potential for Their Adaptation in Indonesia

The digital revolution of the 21st century has brought profound challenges to criminal justice systems worldwide.⁵² Digital platforms have increasingly become the medium for crimes, particularly offences including child sexual exploitation. Growing digital use prompted states to reconsider traditional models of punishment.⁵³ Conventional penalties such as imprisonment or fines were often insufficient to prevent recidivism when offenders continued to have

⁴⁹ Kelly M. Babchishin, R. Karl Hanson, and Chantal A. Hermann, "The Characteristics of Online Sex Offenders: A Meta-Analysis," *Sexual Abuse* 23, no. 1 (March 26, 2011): 92–123, <https://doi.org/10.1177/1079063210370708>.

⁵⁰ Ethel Quayle, "Prevention, Disruption and Deterrence of Online Child Sexual Exploitation and Abuse," *ERA Forum* 21, no. 3 (December 2020): 429–47, <https://doi.org/10.1007/S12027-020-00625-7/METRCS>.

⁵¹ Eva Lievens, *The International Encyclopedia of Digital Communication and Society*, ed. Peng Hwa Ang and Robin Mansell, *The International Encyclopedia of Digital Communication and Society* (Wiley, 2015), <https://doi.org/10.1002/9781118767771>.

⁵² Agrey Kapinga, "The Digital Transformation of Tanzania's Criminal Justice System: Opportunities and Challenges in the Tech Age," *SSRN Electronic Journal*, May 2024, 1–5, <https://doi.org/10.2139/SSRN.4827219>.

⁵³ Nicola Henry and Anastasia Powell, "Sexual Violence in the Digital Age," *Social & Legal Studies* 25, no. 4 (August 12, 2016): 397–418, <https://doi.org/10.1177/0964663915624273>.

unrestricted access to the very tools they used to commit crimes. In response, many jurisdictions developed digital sanctions, including restrictions on internet access, bans on specific apps, or social media blacklisting, as innovative forms of punishment aligned with the digital age.

From a comparative legal perspective, digital sanctions were implemented differently across jurisdictions, shaped by each country's legal tradition, institutional capacity, and sociopolitical context. Although the doctrinal foundations vary, these comparative models offered valuable normative and structural references, such as Indonesia, which was s grappling with a surge in technology-facilitated child sexual offences and lacked comprehensive regulatory mechanisms.

Comparative analysis in this section was based on five parameters: the legal basis for digital restrictions, the scope of prohibited digital conduct, the authority responsible for imposing and supervising the sanction, constitutional or human rights safeguards attached to the restriction, and the restriction's adaptability within Indonesia's criminal justice system. These parameters were important because social media blacklisting could not be assessed merely by asking whether other countries have adopted similar measures. It must be examined in terms of legality, proportionality, enforceability, and compatibility with the broader philosophy of punishment. Selected jurisdictions represented different regulatory models across five legal systems. The United Kingdom reflected a risk-based judicial order model; the United States illustrated constitutional limits on overbroad restrictions; South Korea adopted intensive preventive monitoring; Germany used administrative and multi-stakeholder enforcement; and Sweden and Norway integrated digital monitoring within rehabilitation and reintegration frameworks.

Table 1. Comparative Table of Digital Sanctions in Selected Jurisdictions

Jurisdiction	Legal Mechanism	Sanction Scope	Legal Philosophy	Key Features
United Kingdom	Sexual Harm Prevention Orders (SHPOs)	Device, app, and social media restrictions based on risk	Risk-based, individualised sentencing	Reviewed by courts and probation officers
United States	State-level digital restrictions	Prohibitions on social media use must be narrowly tailored	Proportionality & constitutional limits (1st Amendment)	NC sets constitutional standard
South Korea	Ankle bracelets, registry, and app bans	Comprehensive bans + monitoring + public registry	Preventive justice; utilitarian focus	Electronic monitoring + public awareness
Germany	Internetsperre & behavioural orders	Administrative and probation-related digital bans	Collaborative enforcement; regulatory approach	Cooperation with ISPs and regulators

Sweden & Norway	Digital behaviour monitoring	Conditional access; behavioural therapy; structured reintegration	Rehabilitative-integrative penal policy	Psychological oversight and reintegration support
-----------------	------------------------------	---	---	---

Source: Processed from various sources

Based on Table 1, digital sanctions across comparative legal systems did not operate under a single, uniform model. The United Kingdom adopted a risk-based, individualised sentencing model through Sexual Harm Prevention Orders. Meanwhile, the United States showed the constitutional limits of digital restrictions by requiring that any social media ban be narrowly designed and proportionate. South Korea adopted a more intensive preventive model through offender registration, electronic monitoring, and public awareness mechanisms. Germany focused on collaborative enforcement, including courts, administrative authorities, regulators, and internet service providers. Sweden and Norway placed digital monitoring within a broader rehabilitative and reintegrative penal framework. The comparative results showed that social media blacklisting could be adapted in Indonesia only when it was supported by three safeguards, namely a clear statutory basis, individualised judicial assessment, and technologically feasible post-sentence supervision.

In the United Kingdom, a developed framework for digital sanctions could be found in the use of SHPOs,⁵⁴ which were court-issued orders imposed on individuals who have committed or tended to commit sexual offenses. Judicial orders permit restrictions on a range of behaviours, including digital activities. Restrictions prohibited the offender from owning certain devices, using specific applications, or maintaining anonymous accounts on social media platforms. SHPOs were designed to each individual's risk profile and were regularly reviewed by supervising authorities, including police and probation services. This model showed a risk-based sentencing method in which penalties were designed not solely in reaction to past offences but were also preventive in nature. SHPOs were consistent with the principle of individualised sentencing, which required consideration of the offender's behaviour, risk level, and context in determining suitable sanctions. By restricting digital activity, the law directly targeted the tools and environments used to commit crimes, reinforcing the protective function of punishment in modern legal systems.

The United States adopted a decentralised method due to its federal structure. Individual states have the authority to enact digital restrictions independently. In Florida and California, laws prohibited convicted sex offenders from using social

⁵⁴ Andrew Scholey and Pooneh Bagheri Zadeh, "A Digital Forensics Live Suspicious Activity Toolkit To Assist Investigators With Sexual Harm Prevention Order Monitoring," *5th IEEE Conference on Dependable and Secure Computing, DSC 2022 and SECSOC 2022 Workshop, PASS4IoT 2022 Workshop SICSIA International Paper/Poster Competition in Cybersecurity*, 2022, 1–5, <https://doi.org/10.1109/DSC54232.2022.9888937>.

media or interacting online with minors. However, this method raised constitutional concerns, particularly in light of the First Amendment, which guaranteed freedom of expression. In the landmark case of *Packingham v. North Carolina* (2017), the U.S. Supreme Court struck down a law that broadly banned registered sex offenders from accessing social media platforms, ruling it overly broad and unconstitutional.⁵⁵ Despite invalidating the North Carolina statute, the Court acknowledged that narrowly designed digital restrictions serving a compelling interest, including child protection, remained legally permissible. This case showed the importance of the principle of proportionality in punishment. Digital sanctions, including social media blacklisting, require careful formulation to avoid unnecessary infringement on fundamental rights. Appropriate scope limitations and evidence of ongoing risk support legal validity.

The lesson from *Packingham* was particularly important for Indonesia. The case did not support a blanket prohibition on social media use by all convicted offenders. However, it warned that broad, indefinite, and undifferentiated restrictions could violate fundamental rights because social media was an essential forum for expression, information, employment, education, and civic participation. Therefore, the Indonesian model should avoid a general ban that disconnects offenders entirely from the digital world. A constitutionally safer method was to authorize courts to impose narrowly designed restrictions based on the offender's specific conduct, the platform used to commit the crime, the risk of reoffending, and the need to protect child victims. This showed that social media blacklisting should operate as an individualised judicial order, not as an automatic consequence of conviction.

In South Korea, digital sanctions formed part of a comprehensive, highly structured method for combating sexual offences. The government mandated that convicted child sex offenders register their addresses, wear electronic monitoring devices (ankle bracelets), and refrain from employment in child-related sectors.⁵⁶ Offenders should also be restricted from using specific applications or online platforms. Furthermore, South Korea maintained a public registry that published identifying information about convicted offenders, enabling community-level awareness and vigilance. This multi-pronged system was credited with reducing recidivism rates and strengthening public trust in state protection. The South Korean model exemplified the doctrine of preventive justice, whereby legal interventions were not only reactive but also anticipatory. The system used legal authority to limit offenders' access to environments and tools that may facilitate reoffending. This method was grounded in utilitarian penal theory, which prioritised the community's welfare and safety over retributive principles. The

⁵⁵ Michael L. Smith, "Social Media Regulation and Expressive Conduct After 303 Creative and NetChoice," *SSRN Electronic Journal*, February 2024, 1–51, <https://doi.org/10.2139/SSRN.4738339>.

⁵⁶ Ahn, Han, and Choi, "Reassessing Residency Restrictions: Analyzing Crime Proximity and Patterns for Sex Offenders in South Korea."

integration of digital restrictions into rehabilitation programs showed an evolving understanding of how to address technologically facilitated harm.

In Germany, the method of digital restrictions was less punitive and more administrative. Although German criminal law permitted the imposition of behavioural orders on offenders, digital access restrictions were often enacted through regulatory and administrative channels rather than direct sentencing. A notable tool was the Internetsperre, or internet blocking mechanism, which was used to prevent access to illegal online content, such as child pornography. Courts imposed bans on the use of internet services during probation or post-release monitoring, particularly when offences involved digital communication or distribution. Germany's model showed the importance of collaborative enforcement, wherein legal enforcement was shared between the state, regulatory bodies, and private technology companies. Internet service providers, hosting platforms, and digital intermediaries were integrated into the enforcement chain to ensure compliance with court orders. This showed a shift toward a multi-stakeholder model of digital governance, recognising that effective crime prevention in cyberspace required active cooperation between legal institutions and technological infrastructure.

Scandinavian countries such as Sweden and Norway used digital sanctions within penal systems, but with a focus on offender rehabilitation and reintegration.⁵⁷ Offenders in these jurisdictions were required to participate in digital behaviour monitoring programs, often including real-time oversight of internet activity, counselling, and structured reintegration plans. These measures were accompanied by legal agreements outlining acceptable digital conduct and could include temporarily suspending access to certain platforms or communication tools during the monitoring period.

The Scandinavian method demonstrated an integrated penal policy that combined elements of punishment, social work, technological oversight, and psychological intervention.⁵⁸ Digital sanctions were not treated as purely retributive tools but as part of a broader strategy to reshape offenders' social behaviour and reduce future risks. By rooting digital restrictions within rehabilitative frameworks, these countries showed that punishment and social reintegration need not be in conflict but can be complementary goals.

The adoption feasibility of digital sanction models within Indonesia's national criminal justice system required careful assessment. Indonesia's legal framework followed the civil law tradition, allowing statutory development and doctrinal innovation. Although the new Indonesian Penal Code (KUHP 2023) introduced updates to traditional criminal norms, it did not explicitly recognise digital

⁵⁷ Tapio Lappi-Seppälä, "Penal Policy in Scandinavia," *Crime and Justice* 36, no. 1 (January 2007): 217–95, <https://doi.org/10.1086/592812>.

⁵⁸ Peter Scharff Smith and Thomas Ugelvik, "Punishment and Welfare in Scandinavia," in *Palgrave Studies in Prisons and Penology* (Palgrave Macmillan, London, 2017), 511–29, https://doi.org/10.1057/978-1-137-58529-5_21.

restrictions or social media blacklisting as ancillary penalties. The Draft Criminal Procedure Code (RKUHAP) also lacked mechanisms that would allow courts to impose and monitor digital access bans.

The first step toward adaptation would include normative reconstruction of sentencing provisions to explicitly authorise courts to impose digital restrictions on offenders, particularly in cases involving online child sexual exploitation. This reform could be achieved through legislative amendments to the KUHP or by enacting specialised child protection regulations that integrate digital sanctions into sentencing frameworks. The process remained consistent with the broader principle of contextual criminal justice, where punishment reflects the realities and risks of the digital environment.

Institutional capacity remains another critical factor, as the successful implementation of digital sanctions requires digital forensic units, judicial officers and prosecutors with digital literacy, and operational cooperation with platform providers. Therefore, Indonesia must prioritise capacity building for law enforcement agencies, including establishing cyber units to monitor offenders' compliance with digital restrictions. Without adequate technological infrastructure, any reform risks becoming symbolic or unenforceable. Societal readiness also remains crucial because public understanding and acceptance of digital sanctions strengthen legitimacy and effectiveness. In communities where digital risks were poorly understood, sanctions such as social media bans were perceived as trivial or unnecessary. Public education campaigns must accompany legal reforms, raising awareness of the relationship between online access and the risk of child victimisation, and explaining how digital sanctions serve a protective function.

Adaptation of digital sanctions at the philosophical level must remain consistent with Indonesia's constitutional and moral values. The national commitment to child protection, enshrined in Article 28B (2) of the 1945 Constitution and reinforced by ratification of the Convention on the Rights of the Child, provided a strong normative basis for legal innovation. The best interests of the child principle must guide all policy and sentencing decisions, including digital sexual crimes, ensuring that justice is not only punitive but protective.⁵⁹ Comparative models showed that digital sanctions extended beyond theoretical possibilities and functioned as proven instruments of contemporary criminal justice. Structural, legal, and cultural differences required careful consideration, yet the underlying goal remained universal, preventing offenders from returning to the same digital spaces used for criminal activities. Indonesia could learn from these international practices to design a hybrid model that reflects domestic values while embracing global best practices.

⁵⁹ Aryadi Almau Dudy and Suheflihusnaini Ashady, "Principles of Child Protection in the National Criminal Code: Law Number 1 of 2023," *JIHAD: Jurnal Ilmu Hukum Dan Administrasi* 6, no. 4 (December 2024): 2745–9489, <https://doi.org/10.58258/JIHAD.V6I4.7874>.

Formulating Social Media Blacklisting as an Additional Criminal Sanction in Indonesia's Criminal Justice System

The need for sentencing reform in response to child sexual abuse facilitated through digital platforms prompted important innovations in penal policy, such as the introduction of social media blacklisting as an additional criminal sanction. In this context, offenders may be prohibited from accessing, owning, or using specific social media platforms either temporarily or permanently as part of the sentence. Within Indonesia's current legal reform, particularly the enactment of the 2023 National Criminal Code (KUHP), this concept was highly relevant as a legal and policy response to the growing challenges posed by technology-facilitated sexual crimes against children. Under the Indonesian penal system, as structured in Articles 64 to 68 of the KUHP 2023, criminal sanctions were divided into principal and additional penalties, including revocation of certain rights, confiscation of property, and the publication of judgments. However, no provision explicitly permits digital access restrictions or social media bans as additional punishment. This caused a normative gap in addressing technology-driven offences, particularly child sexual abuse committed through digital communication or social platforms.

The structure of Articles 64 to 68 of the KUHP 2023 provided an entry point for developing social media blacklisting as an additional punishment, but it does not establish a sufficient legal basis for its direct application. The principle of legality requires that any criminal sanction affecting individual liberty and constitutional rights must be clearly prescribed by law. Therefore, social media blacklisting cannot be imposed through expansive judicial interpretation of existing additional penalties. It must be expressly formulated either as a new type of additional punishment or as a specific additional measure applicable to crimes committed through electronic systems, particularly offences including child sexual exploitation. The placement as an additional punishment was doctrinally appropriate because it did not replace imprisonment or fines but complemented these punishments by targeting the digital means the offender used to commit or repeat the crime.

A comprehension of the legal foundation of supplementary punishment was necessary to establish social media blacklisting as a legitimate form of additional sanction in Indonesia. Theoretically, additional sanctions were intended to complement principal punishments in achieving more proportionate and effective penal outcomes. In modern penal theory, supplementary penalties must be rational, contextual, and socially protective. In cases including sexual exploitation of minors through social media, banning the offender from digital platforms was not simply a restriction of rights but a logical legal intervention targeting the means through which the crime was committed.

The *ultimum remedium* principle within Indonesian criminal law supported the application of additional sanctions selectively to serious crimes with substantial societal and victim impact. Social media blacklisting, when designed proportionately

and for a limited scope, served preventive, retributive, and rehabilitative purposes. It was consistent with the principle of subsidiarity in criminal law, which mandated that penal interventions be reserved for cases where other legal remedies were insufficient. Normatively, social media blacklisting could be included among the additional punishments under Article 66 of the KUHP. A possible legislative formulation might read: *“Prohibition against accessing or using specified digital platforms, including social media, for a period determined by the court, in cases where such platforms were used as tools to commit a criminal offence.”* This formulation allowed judicial discretion while maintaining legal clarity and precision.

A more precise legislative formulation may read as follows: “In the event that a criminal offence against a child was committed by using social media, electronic communication platforms, or other digital systems, the court could impose an additional punishment in the form of a prohibition on accessing, developing, operating, or using specified social media accounts or digital platforms for a certain period. The prohibition should be imposed based on the seriousness of the offence, the relationship between the platform and the criminal act, the risk of reoffending, the best interests of the child, and the principle of proportionality. The court should determine the scope, duration, supervisory authority, and legal consequences of violation of such prohibition.” This formulation was preferable due to the ability to clarify the subject, object, legal basis, judicial authority, criteria of imposition, and safeguards against excessive restrictions.

The principle of legality must serve as the primary safeguard in the formulation of social media blacklisting. Access restrictions on digital communication require clear statutory regulation governing elements, scope, duration, supervisory mechanisms, and consequences of violations before judicial imposition. Judicial creativity alone cannot establish a new form of criminal sanction because criminal punishment must remain predictable and accessible before it is applied. In this regard, the role of the legislature was central. The legislature needs to determine whether social media blacklisting will be inserted into the KUHP as a general additional punishment, into the Child Protection Law or Sexual Violence Crime Law as a special additional punishment, or into a future criminal procedure reform as a post-conviction supervisory order. Without this statutory basis, the sanction risked violating the legality principle and undermining legal certainty. This provision could be reinforced by implementing regulations, possibly through a Government Regulation or a Supreme Court Regulation. The instruments should define evidentiary standards, enforcement procedures, monitoring mechanisms, and post-sentence supervision. For instance, offenders could be required to register their digital accounts with monitoring agencies or be subject to periodic inspections by cyber police. These mechanisms would reflect practices in other jurisdictions that apply risk-based sentencing frameworks.

Based on a doctrinal perspective, the introduction of social media blacklisting must remain consistent with Indonesia’s constitutional protections. Articles 28D and 28F of the 1945 Constitution guarantee individual rights to information and

expression. Therefore, any sanction, including digital restrictions, must be narrowly designed, applied only to offenders proven to have misused digital platforms for serious crimes, and supported by evidence of high risk of recidivism. In this regard, restrictions must be *judicially tailored and grounded* in a court ruling based on case-specific findings.

Courts need to apply a proportionality test before imposing social media blacklisting to avoid unconstitutional interference with digital rights. First, the sanction must pursue a legitimate aim, namely the protection of children from repeated sexual exploitation in digital spaces. Second, it must be necessary, implying that less restrictive measures would be insufficient to prevent the offender from reusing digital platforms to reach or exploit children. Third, it must be proportionate in the strict sense, requiring a balance between the seriousness of the risk posed by the offender and the degree of restriction imposed. This test required courts to avoid total, permanent, and platform-wide bans unless the restrictions were strictly justified by the facts of the case. The preferred model was a limited, individualised, and reviewable restriction that targeted the specific digital conduct connected to the offence.

The principle of proportionality was essential to ensuring that the sanctions did not violate fundamental rights while still achieving a protective purpose. Courts should be empowered to determine the scope and duration of the ban and to specify which platforms are included. For example, an offender who used TikTok to exploit a child should not automatically be banned from all digital platforms indefinitely. This method balanced societal protection with respect for the offender's civil liberties. Operationalising the sanctions also required coordinated participation of state institutions and digital intermediaries. Implementation could not succeed without collaboration with major service providers, such as Meta (Facebook, Instagram, WhatsApp), ByteDance (TikTok), or Telegram. The government must develop digital cooperation protocols through memoranda of understanding or binding regulations, enabling state authorities to request platform-based enforcement and conduct digital identity verification. This effort must also be supported by digital forensic capabilities. The Indonesian National Police Cybercrime Unit must be equipped with specialised software to monitor compliance with court-ordered social media bans. Offender's violation of the ban could result in extended restrictions or new contempt-of-court charges. Adequate legal and technical infrastructure can support social media blacklisting as an enforceable and effective deterrent measure.

Progressive penal theory viewed punishment as extending beyond retribution or incapacitation to include social protection and risk prevention.⁶⁰ In this sense, penalties for perpetrators of child sexual abuse should focus on minimising the

⁶⁰ Reid Griffith Fontaine, "Social Information Processing, Subtypes of Violence, and a Progressive Construction of Culpability and Punishment in Juvenile Justice," *International Journal of Law and Psychiatry* 31, no. 2 (March 2008): 136–49, <https://doi.org/10.1016/J.IJLP.2008.02.002>.

likelihood of repeat contact with victims, whether physically or digitally.⁶¹ Social media blacklisting offered a penalty model that was protective rather than purely punitive. This prevented offenders from re-engaging with the digital spaces previously used to commit harm. The normative construction was also consistent with the best interests of the principle, enshrined both in international law and Indonesia's domestic legal system. As a signatory to the CRC, Indonesia was obliged to take all appropriate measures to protect children from exploitation, including in digital environments. In this context, digital access restrictions become a penal option and a constitutional duty to safeguard children's rights.

Academically, the developing literature supported the development of technology-based punishment, particularly the concept of digital incapacitation. This method reframed the idea of punishment from just physical confinement to the deprivation of technological capacity used for criminal activity. Theories of *digital-specific punishment* have gained traction in European and North American criminal justice scholarship and were increasingly discussed in developing contexts like Brazil, India, and Indonesia. Social media blacklisting fits squarely within this theoretical framework. A compelling argument for integrating this sanction into Indonesian law was the inadequacy of traditional penalties for addressing digital recidivism. Even after serving a prison sentence, offenders often retained full access to social media platforms, thereby posing continued threats to children. Therefore, social media blacklisting should be viewed not just as an add-on to prison terms, but as a post-penal control mechanism necessary for long-term protection. This model also resonated with situational crime prevention theory, which focused on reducing opportunities for criminal behaviour by restricting offender access to tools or environments that facilitate crime. In this case, digital platforms were the tools, and removing the access significantly reduced the potential for reoffending. This method differentiated between punishing behaviour and preventing harm, both of which were legitimate aims of a modern criminal justice system.

Incorporating social media blacklisting into sentencing would necessitate procedural updates within criminal procedure law. Currently, Indonesia's Criminal Procedure Code (KUHP) does not authorise prosecutors or judges to request or impose digital access bans. Therefore, a legal basis must first be established at the statutory level, followed by procedural rules outlining how such bans are to be imposed, monitored, and enforced.

Digital risk assessment remained essential because Indonesia should consider establishing a digital risk assessment authority similar to models adopted in the United Kingdom and Canada. These bodies assessed the tendency of reoffending and recommended appropriate restrictions. Through the assessments, courts could

⁶¹ Luciana C Assini-Meytin, Rebecca L Fix, and Elizabeth J Letourneau, "Child Sexual Abuse: The Need for a Perpetration Prevention Focus," *Journal of Child Sexual Abuse* 29, no. 1 (January 2020): 22–40, <https://doi.org/10.1080/10538712.2019.1703232>.

issue more scientifically grounded and individualised orders, ensuring that digital sanctions were evidence-based and proportionate. Consideration of normative, doctrinal, institutional, and technical aspects showed that social media blacklisting constituted a viable and urgent additional sanction within Indonesia's criminal justice landscape. It was a concrete response to technology-facilitated child sexual crimes and offered a legal mechanism that was preventive, enforceable, and constitutionally aligned.

Conclusion

In conclusion, the transformation of digital society has changed the modus operandi of sexual crimes against children. Offenders no longer depend on physical proximity, but increasingly use social media, anonymous accounts, encrypted communication, and digital manipulation to groom, exploit, and control child victims. This development exposes the inadequacy of conventional sentencing models that depend primarily on imprisonment and fines. Existing criminal penalties remain necessary, yet post-conviction offender access to digital platforms used for criminal activities remains unaddressed. Therefore, sentencing reform is urgently needed to ensure that criminal punishment responds to past wrongdoing and future risk of digital recidivism.

Comparative legal systems show that criminal justice frameworks can incorporate digital restrictions through clear legal safeguards. The United Kingdom offers a risk-based judicial order model, the United States provides an important constitutional warning against blanket restrictions, South Korea uses intensive preventive monitoring, Germany focuses on multi-stakeholder enforcement, and Scandinavian jurisdictions show the value of combining digital supervision with rehabilitation. These models show that social media blacklisting should not be understood as a general ban on digital life, but as a targeted additional punishment imposed by courts when there is a clear connection between the offence, the offender's digital conduct, and the need to protect children.

In the context of Indonesia, social media blacklisting should be formulated as an additional criminal sanction with a clear statutory basis, preferably through amendments to the KUHP, the Child Protection Law, the Sexual Violence Crime Law, and procedural rules in the KUHAP or implementing regulations. The sanction must be imposed only by judicial decision, limited in scope and duration, based on individual risk assessment, and subject to proportionality review. Its implementation requires cooperation among courts, prosecutors, police cyber units, correctional/probation authorities, child protection institutions, the Ministry of Communication and Digital Affairs, and digital platform providers. Clear legal safeguards can support social media blacklisting as a constitutionally acceptable and practically relevant instrument of penal reform for protecting children, preventing repeat offending, and strengthening Indonesia's criminal justice response to technology-facilitated sexual crimes.

References

- Aguirre, Alejandro Herrán. “Derecho a La Libertad de Expresión y Acceso a Las Redes Sociales: El Caso Packingham Con Carolina Del Norte.” *Revista Chilena de Derecho y Tecnología* 7, no. 2 (December 2018): 163–86. <https://doi.org/10.5354/0719-2584.2018.49020>.
- Ahn, Jaekyung, Sung Yon Han, and Yimoon Choi. “Reassessing Residency Restrictions: Analyzing Crime Proximity and Patterns for Sex Offenders in South Korea.” *International Journal of Offender Therapy and Comparative Criminology* 69, no. 10–11 (August 2025): 1524–43. <https://doi.org/10.1177/0306624X251317575>.
- Ali, Mahrus, Zico Junius Fernando, Chairul Huda, and Mahmutarom Mahmutarom. “Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims.” *Substantive Justice International Journal of Law* 8, no. 1 (May 2025): 1–12. <https://doi.org/10.56087/SUBSTANTIVEJUSTICE.V8I1.306>.
- Aprianto, Sandi, and Widya Timur. “Juridical Review of the Role of Society Against Sexual Crimes of Minors Through Gadgets Based on Law Number 19 of 2016 Concerning Information and Electronic Transactions.” *JURNAL HUKUM SEHLASEN* 9, no. 1 (April 2023): 41–50–41 – 50. <https://doi.org/10.37676/JHS.V9I1.3893>.
- Arifin, Zainal, Zico Junius Fernando, and Emi Puasa Handayani. “Implikasi Hukum Perubahan Kedua Undang-Undang Informasi Dan Transaksi Elektronik: Menyeimbangkan Kebebasan Berpendapat Dan Partisipasi Publik Dalam Demokrasi Digital: Legal Implications of The Second Amendment to The Electronic Information and Transactions Law: Balancing Freedom of Expression and Public Participation in Digital Democracy.” *LITIGASI* 26, no. 1 (April 2025): 192–227. <https://doi.org/10.23969/LITIGASI.V26I1.21555>.
- Assini-Meytin, Luciana C, Rebecca L Fix, and Elizabeth J Letourneau. “Child Sexual Abuse: The Need for a Perpetration Prevention Focus.” *Journal of Child Sexual Abuse* 29, no. 1 (January 2020): 22–40. <https://doi.org/10.1080/10538712.2019.1703232>.
- Babchishin, Kelly M., R. Karl Hanson, and Chantal A. Hermann. “The Characteristics of Online Sex Offenders: A Meta-Analysis.” *Sexual Abuse* 23, no. 1 (March 26, 2011): 92–123. <https://doi.org/10.1177/1079063210370708>.
- Behfar, Arezou, Ankit Shrestha, and Mahdi Nasrullah Al-Ameen. “A First Look into Fake Profiles on Social Media through the Lens of Victim’s Experiences.” In *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing*, 444–50. New York, NY, USA: ACM, 2024. <https://doi.org/10.1145/3678884.3681889>.
- Bjelajac, Željko Đ., and Aleksandar M. Filipović. “Flexibility of Digital Media for Manipulative Activities of Sexual Predators.” *KULTURA POLISA* 18, no.

- 44 (March 2021): 51–67.
<https://doi.org/10.51738/KPOLISA2021.18.1R.2.01>.
- Broadhurst, Roderic. *Child Sex Abuse Images and Exploitation Materials. The Human Factor of Cybercrime*. Routledge, 2019.
<https://doi.org/10.4324/9780429460593-14>.
- Choi, Kyung-Shick, and Hannarae Lee. “The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response.” *Journal of Child Sexual Abuse*, n.d., 1–20.
<https://doi.org/10.1080/10538712.2023.2214540>.
- Chung, Woo Sik. “An Empirical Validation of a Theory of Punishment.” *International Journal of Comparative and Applied Criminal Justice* 18, no. 1–2 (January 1994): 221–48.
<https://doi.org/10.1080/01924036.1994.9689039>.
- Dewi, Anita Permata. “KPAI: HAN 2024 Momentum Lindungi Anak Di Ranah Daring.” ANTARA News, 2024.
- Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P Suzor, Delanie Woodlock, and Bridget Harris. “Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms.” *Feminist Media Studies* 18, no. 4 (July 2018): 609–25. <https://doi.org/10.1080/14680777.2018.1447341>.
- Dudy, Aryadi Almau, and Suheflihusnaini Ashady. “Principles of Child Protection in the National Criminal Code: Law Number 1 of 2023.” *JIHAD: Jurnal Ilmu Hukum Dan Administrasi* 6, no. 4 (December 2024): 2745–9489. <https://doi.org/10.58258/JIHAD.V6I4.7874>.
- Ega, Ni Putu, and Maha Wiryanthi. “Copyright Infringement in Online Media: Corporate Legal Liability.” *Al-Adalah: Jurnal Hukum Dan Politik Islam* 10, no. 1 (January 2025): 151–67.
<https://doi.org/10.30863/AJMPI.V10I1.7681>.
- Fernando, Zico Junius, Pujiyono, Umi Rozah, and Nur Rochaeti. “The Freedom of Expression in Indonesia.” *Cogent Social Sciences* 8, no. 1 (July 2022): 1–11.
<https://doi.org/10.1080/23311886.2022.2103944>.
- Fontaine, Reid Griffith. “Social Information Processing, Subtypes of Violence, and a Progressive Construction of Culpability and Punishment in Juvenile Justice.” *International Journal of Law and Psychiatry* 31, no. 2 (March 2008): 136–49. <https://doi.org/10.1016/J.IJLP.2008.02.002>.
- Handayani, Emi Puasa, Zainal Arifin, and Zico Junius Fernando. “Criminal Penalties in Cyberspace: Between the Development of Digital Democracy and Authoritarianism.” *Indonesian Journal of Criminal Law Studies* 10, no. 1 (May 2025): 45–82. <https://doi.org/10.15294/IJCLS.V10I1.19652>.
- Helsper, Ellen Johanna, and David Smahel. “Excessive Internet Use by Young Europeans: Psychological Vulnerability and Digital Literacy?” *Information, Communication & Society* 23, no. 9 (July 2020): 1255–73.
<https://doi.org/10.1080/1369118X.2018.1563203>.

- Henry, Nicola, and Anastasia Powell. "Sexual Violence in the Digital Age." *Social & Legal Studies* 25, no. 4 (August 12, 2016): 397–418. <https://doi.org/10.1177/0964663915624273>.
- Henshaw, Marie, James R P Ogloff, and Jonathan A. Clough. "Demographic, Mental Health, and Offending Characteristics of Online Child Exploitation Material Offenders: A Comparison with Contact-only and Dual Sexual Offenders." *Behavioral Sciences & the Law* 36, no. 2 (March 16, 2018): 198–215. <https://doi.org/10.1002/bsl.2337>.
- Horsman, Graeme. "Reviewing the Devices of Those Subject to Sexual Harm Prevention Orders (SHPOs): IOS Opportunities, Limitations and Strategies." *Australian Journal of Forensic Sciences* 57, no. 1 (January 2025): 16–38. <https://doi.org/10.1080/00450618.2023.2252472>.
- Joleby, Malin, Carolina Lunde, Sara Landström, and Linda S. Jonsson. "Offender Strategies for Engaging Children in Online Sexual Activity." *Child Abuse & Neglect* 120 (October 2021): 1–5. <https://doi.org/10.1016/J.CHIABU.2021.105214>.
- Judijanto, Loso, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights* 3, no. 01 (October 2024): 20–29. <https://doi.org/10.58812/ESLHR.V3I01.351>.
- Kapinga, Agrey. "The Digital Transformation of Tanzania's Criminal Justice System: Opportunities and Challenges in the Tech Age." *SSRN Electronic Journal*, May 2024, 1–5. <https://doi.org/10.2139/SSRN.4827219>.
- Kingston, Sarah, and Terry Thomas. "The Sexual Risk Order and the Sexual Harm Prevention Order." *Probation Journal* 65, no. 1 (March 7, 2018): 77–88. <https://doi.org/10.1177/0264550517748359>.
- Kloess, Juliane A., Sarah Seymour-Smith, Catherine E. Hamilton-Giachritsis, Matthew L. Long, David Shipley, and Anthony R. Beech. "A Qualitative Analysis of Offenders' Modus Operandi in Sexually Exploitative Interactions With Children Online." *Sexual Abuse* 29, no. 6 (September 10, 2017): 563–91. <https://doi.org/10.1177/1079063215612442>.
- Lappi-Seppälä, Tapio. "Penal Policy in Scandinavia." *Crime and Justice* 36, no. 1 (January 2007): 217–95. <https://doi.org/10.1086/592812>.
- Lievens, Eva. *The International Encyclopedia of Digital Communication and Society*. Edited by Peng Hwa Ang and Robin Mansell. *The International Encyclopedia of Digital Communication and Society*. Wiley, 2015. <https://doi.org/10.1002/9781118767771>.
- Livingstone, Sonia, Amanda Third, Patrick Burton, Sabine Witting, Eva Lievens, Stacey Steinberg, Shuli Gilutz, and David Souter. "The UN Committee on the Rights of the Child's General Comment on the Digital Environment." *AoIR Selected Papers of Internet Research*, March 2022, 1–12. <https://doi.org/10.5210/SPIR.V2022I0.12960>.
- Mamak, Kamil. "Cyber Banishment: An Old Sanction for Virtual Spaces."

- Criminal Justice Studies* 36, no. 2 (April 2023): 133–45. <https://doi.org/10.1080/1478601X.2023.2188449>.
- Mukamurera P., Nyiramana. “The Impact of Social Media on Mental Health.” *Research Invention Journal Of Research In Medical Sciences* 4, no. 1 (March 2025): 11–15. <https://doi.org/10.59298/RIJ RMS/2025/411115>.
- Musofiana, Ida, Aji Sudarmaji, and Ira Alia Maerani. “Aspects of Legal Protection for Children from Cybercrime.” *Jurnal Pembaharuan Hukum* 7, no. 3 (December 2020): 201–10. <https://doi.org/10.26532/JPH.V7I3.12820>.
- Panggabean, Andreas Daniel. “Ini Data Statistik Penggunaan Media Sosial Masyarakat Indonesia Tahun 2024.” RRI.co.id, 2024.
- Panjaitan, Ranto Daniel, and Diki Zukriadi. “Pertanggung Jawaban Hukum Terhadap Anak Sebagai Korban Cyberbullying Pada Media Sosial.” *SCIENTIA JOURNAL: Jurnal Ilmiah Mahasiswa* 6, no. 3 (February 2024): 1–10. <https://doi.org/10.33884/SCIENTIAJOURNAL.V6I3.8277>.
- Pujayanti, Luh Putu Vera Astri, Sopian, Herlina Sulaiman, Sahrul, and Misno. “Legal Review of Child Grooming as A Crime of Sexual Violence in Indonesia.” *Jurnal Hukum Dan HAM Wara Sains* 2, no. 03 (March 2023): 188–96. <https://doi.org/10.58812/JHHWS.V2I03.252>.
- Putra, Yagie Sagita, Pujiyono Pujiyono, Nur Rochaeti, and Zico Junius Fernando. “EIT Law at the Crossroads: Exploring Legal Dilemmas, Freedom of Expression, and Human Rights.” *Pakistan Journal of Criminology* 16, no. 3 (July 2024): 1315–32. <https://doi.org/10.62271/PJC.16.3.1315.1332>.
- Putri, Karima Naila, Kiki Kristanto, and Yurika F.Dewi. “Criminal Liability for Indonesians Who Use Digital Wallets to Commit Child Sexual Exploitation.” *Journal of Law, Politic and Humanities* 5, no. 3 (January 2025): 2043–52. <https://doi.org/10.38035/JLPH.V5I3.1434>.
- Quayle, Ethel. “Prevention, Disruption and Deterrence of Online Child Sexual Exploitation and Abuse.” *ERA Forum* 21, no. 3 (December 2020): 429–47. <https://doi.org/10.1007/S12027-020-00625-7/METRICS>.
- Reisdorf, Bianca C., and Yvonne Jewkes. “(B)Locked Sites: Cases of Internet Use in Three British Prisons.” *Information Communication and Society* 19, no. 6 (June 2016): 771–86.
- Rex, Sue. “Punishment as Communication.” In *Alternatives to Prison*, 131–52. Willan, 2013. <https://doi.org/10.4324/9781843925743-12>.
- Scholey, Andrew, and Pooneh Bagheri Zadeh. “A Digital Forensics Live Suspicious Activity Toolkit To Assist Investigators With Sexual Harm Prevention Order Monitoring.” *5th IEEE Conference on Dependable and Secure Computing, DSC 2022 and SECSOC 2022 Workshop, PASS4IoT 2022 Workshop SICSA International Paper/Poster Competition in Cybersecurity, 2022*, 1–5. <https://doi.org/10.1109/DSC54232.2022.9888937>.
- Shaw, Lauren. “A Cross Comparison of Temporary Work Release Programs as an Alternative to Incarceration Within Canada and Ukraine.” *Crossing Borders: Student Reflections on Global Social Issues* 4, no. 1 (November 2022): 1–

10. <https://doi.org/10.31542/CB.V4I1.2478>.
- Smith, Michael L. "Social Media Regulation and Expressive Conduct After 303 Creative and NetChoice." *SSRN Electronic Journal*, February 2024, 1–51. <https://doi.org/10.2139/SSRN.4738339>.
- Smith, Peter Scharff, and Thomas Ugelvik. "Punishment and Welfare in Scandinavia." In *Palgrave Studies in Prisons and Penology*, 511–29. Palgrave Macmillan, London, 2017. https://doi.org/10.1057/978-1-137-58529-5_21.
- Sunkad, Gayatri. "The Impact of Social Media on Society." *International Journal of Social Health* 2, no. 10 (November 2023): 785–91. <https://doi.org/10.58860/IJSH.V2I10.121>.
- Suryandari, Wieke Dewi. "Efforts to Reform Law Enforcement in Tackling Cybercrime." *International Journal of Law Social Sciences and Management* 1, no. 2 (April 2024). <https://doi.org/10.69726/IJLSSM.V1I2.27>.
- Terry, Karen J. "Sex Offender Laws in the United States: Smart Policy or Disproportionate Sanctions?" *International Journal of Comparative and Applied Criminal Justice* 39, no. 2 (April 2015): 113–27. <https://doi.org/10.1080/01924036.2014.973048>.
- Tosza, Stanislaw. "Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors." *Computer Law & Security Review* 43 (November 2021): 1–5. <https://doi.org/10.1016/J.CLSR.2021.105614>.
- Vatria Barasa, Yesya, Ayu Nurmala, Reva Fisalsabila, Deswita Fitriyani, Ariani Galuh Pangastuti, April Laksana, Jl Raya Serang Jakarta Km, Kota Serang, and Banten Korespondensi Penulis. "Pengaruh Human Relations Terhadap Interaksi & Perilaku Remaja Di Media Sosial." *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 1, no. 6 (December 2024): 166–73. <https://doi.org/10.62383/KONSENSUS.V1I6.480>.
- Vilks, Andrejs. "Cybercrime and Sexual Exploitation of Children in E-Environment in the Context of Strengthening Urban and Rural Security." *SHS Web of Conferences* 68 (2019): 1–11. <https://doi.org/10.1051/SHSCONF/20196801010>.
- Wagner, Ben, Matthias C. Kettemann, and Kilian Vieth. *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*. Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations. Edward Elgar Publishing, 2019. <https://doi.org/10.4337/9781785367724>.
- Witting, Sabine K. "Transnational by Default: Online Child Sexual Abuse Respects No Borders." *The International Journal of Children's Rights* 29, no. 3 (August 2021): 731–64. <https://doi.org/10.1163/15718182-29030010>.
- Wolf, Michiel van der. "Legal Control on Social Control of Sex Offenders in the Community: A European Comparative and Human Rights Perspective." *Erasmus Law Review* 9, no. 2 (December 2016): 39–54.

- <https://doi.org/10.5553/ELR.000074>.
- Xu, Yiyin. "Digital Dangers: How Technology Has Transformed Child Sexual Exploitation." *Advances in Education, Humanities and Social Science Research* 13, no. 1 (March 2025): 99–99.
<https://doi.org/10.56028/AEHSSR.13.1.99.2025>.
- Yonatan, Agnes. "Menilik Pengguna Media Sosial Indonesia 2017-2026." data.goodstats.id, 2023.
- Zico Junius Fernando et al. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (June 2025): 1–39.
<https://doi.org/10.15294/ILDISEA.V4I1.20147>.
- Zubaidi, Nabilah Hani Ahmad. "Monitoring Internet Child Pornography (ICP) in Malaysia." *Pertanika Journal of Social Sciences and Humanities* 29 (2021): 185–203. <https://doi.org/10.47836/PJSSH.29.S2.13>.



© 2026 by the authors. Publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/3.0/>).

[This page has intentionally left blank]