Article Title

The Role of the North Sumatra Regional Police in Combating Pornography in the Digital Era: A Criminal Psychology Perspective

Author(s)

Sapani Martua Rambe*
Universitas Labuhanbatu, Indonesia || *martuasapani@gmail.com*
Corresponding Author

Risdalina Risdalina
Universitas Labuhanbatu, Indonesia || *risdalinasiregar@gmail.com*

Indra Kumalasari
Universitas Labuhanbatu, Indonesia || *indrakumalasarim@gmail.com*

ABSTRACT

This research aims to examine the role of the North Sumatra Regional Police in combating cyber-pornography offenses in the digital era from a criminal psychology perspective. Field research and normative juridical methods were employed to collect primary and secondary data. Primary data were obtained through in-depth interviews, while secondary data were gathered through a literature review. The data were analyzed using a descriptive qualitative approach. The results indicate that cyber-pornography offenses in North Sumatra are a complex phenomenon with diverse modus operandi. The North Sumatra Regional Police has implemented comprehensive strategies, including strengthening investigator capacity, utilizing digital forensic technology, educating the public, and collaborating with internet service providers. However, challenges remain, such as substantiating digital evidence, navigating cross-border jurisdiction, and keeping pace with rapid technological advancements. In conclusion, synergy among stakeholders and public participation are crucial. Continuous evaluation and refinement of strategies are necessary to address the ever-evolving dynamics of cybercrime, considering the factors that influence criminal behavior in the digital realm.

Keywords: *Criminal Psychology; Cyber-Pornography; Digital Forensics; Law Enforcement; North Sumatra Regional Police.*

INTRODUCTION

The digital revolution, characterized by the massive penetration of the internet and social media, has fundamentally reshaped the landscape of interaction and information dissemination in the modern era (Suhyana et al., 2021). However, alongside the convenience and efficiency it offers, this technological advancement has also created an environment conducive to the proliferation of cybercrimes, including the widespread distribution of illicit pornographic content (Rivanie et al., 2021). The complexity of this cybercrime phenomenon is exacerbated by the inherent characteristics of cyberspace, which offer anonymity, broad accessibility, and a constantly evolving array of digital platforms (O'Malley & Holt, 2022). This situation presents substantial challenges for law enforcement agencies across various nations, including Indonesia, underscoring the urgent need to develop comprehensive and adaptive countermeasures.

In response to the increasingly alarming phenomenon of cybercrime, the Indonesian government has enacted comprehensive regulations, namely Law Number 11 of 2008 and Law Number 44 of 2008. These statutes are specifically designed to combat the dissemination of pornographic content in the digital realm. Nevertheless, the implementation of these regulations faces significant obstacles.

The intricacies of enforcing laws against cyber-pornography are compounded by the perpetrators' ability to exploit legal loopholes and leverage sophisticated technologies, such as cloud-based applications and encrypted communications, to evade detection and apprehension (Boopathi & Sneka, 2024). Furthermore, the often

transnational nature of cybercrimes, coupled with the difficulties in collecting and verifying digital evidence, constitutes significant impediments to the law enforcement process (Tombolotutu et al., 2024). Consequently, more effective and comprehensive law enforcement strategies are imperative.

As one of the provinces with a high digital penetration rate, North Sumatra faces increasingly complex challenges in combating cyber-pornography. In this context, the North Sumatra Regional Police, as the leading law enforcement institution in the region, bears a crucial responsibility to adapt and develop effective strategies in response to the ever-evolving dynamics of cybercrime. The success of efforts to prevent and prosecute these crimes depends heavily on inter-agency synergy, enhanced human resource capacity, and the mastery and utilization of cutting-edge digital forensic technology.

Beyond the technical and legal aspects, addressing cybercrimes, particularly those related to pornographic content, requires consideration of broader dimensions, namely their implications for morality and social cohesion. The dissemination of pornographic content in the digital sphere not only constitutes a legal offense but also has the potential to degrade moral values and threaten the social fabric. The destructive impact, especially on victims of exploitation, underscores the importance of a holistic and multidisciplinary approach to this issue.

A thorough understanding of the determining factors that drive criminal behavior in the digital realm is crucial for formulating effective countermeasures. By examining perpetrators' motives and modus operandi, it is anticipated that more targeted prevention and enforcement measures can be identified. In this context, a comprehensive approach is required, including insights from the criminal psychology field (Nugroho et al., 2024).

Based on the foregoing elaboration, this research aims to comprehensively examine the role of the North Sumatra Regional Police in combating pornography-related offenses in the digital era. This study will focus on mapping cyber-pornography patterns in North Sumatra, analyzing the prevailing regulations and law enforcement practices, and evaluating the implemented countermeasure strategies. Through in-depth analysis, taking into account the factors influencing criminal behavior in cyberspace, this research is expected to contribute significantly to developing more effective, adaptive, and responsive cybercrime countermeasure strategies, particularly within the jurisdiction of the North Sumatra Regional Police. The recommendations formulated herein are expected to serve as a strategic reference in creating a secure, dignified, and conducive digital space for all members of society.

METHOD

This research employs a combination of field research and normative juridical methods to comprehensively analyze the role of the North Sumatra Regional Police in combating cyber-pornography offenses in the digital era. A qualitative approach, utilizing field research, is applied to gain an in-depth understanding of the patterns of cyber-pornography occurring within the jurisdiction of the North Sumatra Regional Police (Irwansyah, 2021). Moreover, this method is used to evaluate the effectiveness of the countermeasure strategies implemented by the North Sumatra Regional Police. Concurrently, a normative juridical approach examines and analyzes legislation relevant to pornography-related offenses in the digital era, specifically those forming the legal basis for the North Sumatra Regional Police in carrying out their duties (Qamar & Rezah, 2020).

The data used in this research are derived from primary and secondary sources. Primary data are collected through in-depth interviews with purposively selected informants, comprising police officers within the North Sumatra Regional Police who handle cybercrimes and other relevant parties deemed to possess adequate knowledge and understanding of the research object. These in-depth interviews aim to elicit detailed and comprehensive information regarding the role of the North Sumatra Regional Police in combating cyber-pornography, including the strategies employed, challenges encountered, and achievements to date. Secondary data are obtained through a literature review, examining various legal materials, both primary and secondary, related to the research focus. Primary legal materials include legislation, such as Law Number 11 of 2008 and Law Number 44 of 2008. Secondary legal materials encompass books, scholarly journals, research reports, articles, and other official documents pertinent to the issues under investigation.

All primary and secondary collected data are processed and analyzed qualitatively using a descriptive qualitative technique. Data analysis involves data reduction, data display, and conclusion drawing (Sampara & Husen, 2016). The results of this analysis are then described narratively and systematically to achieve the research objective, which is to illustrate and analyze in depth the role of the North Sumatra Regional Police in combating cyber-pornography in the digital era, taking into account a criminal psychology perspective to understand the behavior of perpetrators and victims, and to formulate constructive recommendations for enhancing the effectiveness of countermeasure efforts against these crimes.

RESULTS AND DISCUSSION

A. Anatomy of Cyber-Pornography Offenses in North Sumatra: Patterns, Modus Operandi, and Targets

The digital landscape in North Sumatra, similar to other regions in Indonesia, is not immune to the shadow of cyber-pornography offenses. This phenomenon is increasingly concerning due to the rising internet penetration and device usage among the public. The complexity of these crimes is demonstrated by the variety of modus operandi, targeted victims, and media utilized by perpetrators. In this context, an in-depth analysis of the anatomy of cyber-pornography offenses in North Sumatra is imperative to formulate effective and comprehensive countermeasure strategies, as well as to understand the factors influencing criminal behavior in these offenses.

Cyber-pornography offenses in North Sumatra manifest through a constantly evolving modus operandi, reflecting the perpetrators' adaptation to technological advancements and regulations. One dominant method involves the utilization of social media platforms as showcases for disseminating pornographic content. The anonymity afforded by these platforms, through features like fake account creation and pseudonyms, is an effective shield for perpetrators to evade legal repercussions (Agustini et al., 2023). Psychologically, they also feel safer and bolder in their actions due to the minimal physical interaction with victims.

Furthermore, these illicit contents are disseminated in various formats, ranging from images and videos to links leading to external pornographic websites. The existence of encryption technologies and Virtual Private Networks (VPNs) further complicates efforts to track and identify perpetrators, underscoring that these offenders are not only adept at exploiting technological loopholes but are also proactive in adopting new methods to avoid detection. These technologies also reflect the perpetrators' understanding of how online systems work and how to evade surveillance.

Vulnerability to cyber-pornography offenses in North Sumatra is not evenly distributed but instead concentrated within specific segments of society. Children and adolescents, who are in a phase of psychological and cognitive development, are primary targets of cyber predators. Their lack of digital literacy and comprehensive understanding of online risks renders them susceptible to manipulation and exploitation. Adolescents and children are often targeted due to their limited understanding of the long-term implications of their online actions.

Perpetrators cunningly employ manipulative persuasion techniques, such as offering gifts or feigning emotional closeness, to lure victims into the web of these crimes. Furthermore, individuals with low digital literacy are also easy targets regardless of age. Their ignorance and negligence in navigating the digital space provide an opening for perpetrators to deploy various fraudulent schemes and exploitative tactics, resulting in material and immaterial damages. It indicates a pattern where perpetrators actively seek out and exploit the psychological vulnerabilities of their victims (Nasrullah, 2023).

The spectrum of digital platforms misused for cyber-pornography offenses in North Sumatra continues to broaden, in line with the rapid pace of technological innovation and shifting trends in social media. Besides mainstream social media platforms like Facebook, Instagram, and Twitter, which are used to reach a broad audience, encrypted instant messaging applications like WhatsApp and Telegram also function as channels for distributing illicit content in a more private and closed manner. The perpetrators' preference for using these private platforms may be driven by a desire for greater control over content distribution and to avoid detection.

The presence of end-to-end encryption features in these applications, while intended to protect user privacy, is also exploited by perpetrators to establish secure communication from surveillance and intervention by law enforcement (Husen et al., 2020). Moreover, the existence of websites and online forums dedicated explicitly to pornographic content, with servers often located outside Indonesian jurisdiction, further complicates efforts to prosecute and eradicate these offenses. These sites are often designed for anonymity and secrecy, aligning with the perpetrators' need to operate outside the reach of the law.

Based on the foregoing, it can be concluded that cyber-pornography offenses in North Sumatra constitute a complex and multidimensional phenomenon. Understanding the anatomy of these crimes, encompassing patterns, modus operandi, targeted victims, and mediums used, is a fundamental step in formulating holistic and sustainable countermeasure strategies. A synergy between strict law enforcement, improved public digital literacy, and developing regulations that adapt to technological advancements is needed to create a safe and conducive digital ecosystem in North Sumatra. Thus, it is hoped that the negative impacts of cyber-pornography offenses can be minimized and optimal protection for all segments of society, especially vulnerable groups, can be realized in this digital era (Salsabilla et al., 2023). This in-depth analysis is also crucial in understanding how the psychological factors of both perpetrators and victims interact with these crimes, providing a basis for more effective interventions.

B. Regulations and Law Enforcement of Cyber-Pornography Offenses: Complexities and Challenges

The increasingly alarming prevalence of cyber-pornography offenses in the digital era, particularly in North Sumatra, demands practical and comprehensive law enforcement. As a legal foundation, Indonesia has Law Number 11 of 2008 and Law Number 44 of 2008. Law Number 11 of 2008 explicitly prohibits the distribution, transmission, and accessibility of electronic content containing pornography. Meanwhile, Law Number 44 of 2008 provides a more specific definition and limitations on prohibited acts related to the production, dissemination, and use of pornography, including those carried out through digital media. These two regulations serve as essential legal instruments for law enforcement agencies, especially the North Sumatra Regional Police, in prosecuting perpetrators of cyber-pornography offenses.

Although normatively, Indonesia has an adequate regulatory framework, field implementation indicates that the enforcement of laws against cyber-pornography offenses still faces various complex obstacles. One of the main challenges encountered by law enforcement agencies, including the North Sumatra Regional Police, relates to the collection and substantiation of digital evidence. In conventional crimes, physical evidence is relatively more straightforward to identify and secure. However, in cybercrime cases, evidence is digital and intangible, making it susceptible to manipulation, deletion, and concealment (Oktana et al., 2023). Perpetrators, for example, can quickly delete digital traces of uploaded pornographic content from servers or utilize technologies like Virtual Private Networks (VPNs) to mask their location and identity, contributing to the difficulty in tracking and identification.

This complexity is further compounded by the dimension of cross-border jurisdiction. Many perpetrators of cyber-pornography offenses operate from abroad or utilize digital platforms based outside Indonesian jurisdiction (Handoyo et al., 2024). Consequently, law enforcement is hindered by procedural and diplomatic obstacles. Indonesian law cannot automatically apply to perpetrators outside its territorial boundaries. Therefore, robust and effective international cooperation between countries and international law enforcement agencies is required. However, regulatory harmonization and differences in legal systems between countries often impede the realization of such cooperation.

Furthermore, the rapid pace of information and communication technology development often surpasses the adaptive capacity of regulations and law enforcement agencies. Perpetrators of cyber-pornography offenses are increasingly adept at exploiting cutting-edge technology to evade detection.

They utilize encrypted messaging applications, platforms prioritizing anonymity, and other sophisticated techniques (Zaltina & Nurtjahyo, 2024). This agility in adopting and adapting to new technologies places law enforcement agencies, including the North Sumatra Regional Police, in a defensive and reactive position. Law enforcement agencies often lag in mastering technology and developing effective digital investigation methods. This gap can be exploited by perpetrators to continue their activities, indicating the need for more proactive and adaptive law enforcement strategies.

Another crucial aspect contributing to the complexity of law enforcement is the limited capacity and capability of human resources in cyber law enforcement (Latifansyah et al., 2024). Although the North Sumatra Regional Police have a special unit assigned to handle cybercrimes, the reality is that not all law enforcement personnel are equipped with adequate technical knowledge and skills in digital forensics, cyber data analysis, and online investigation techniques. These limitations directly impact their effectiveness in identifying, tracking, and proving the involvement of perpetrators in cyber-pornography offenses. The lack of specialized expertise in this area can slow the investigation process and reduce the quality of the evidence gathered.

These various challenges in enforcing laws against cyber-pornography offenses, encompassing technical, juridical, and human resource aspects, are intertwined and form a complex web of problems. A comprehensive understanding of this complex dynamic indicates that addressing cyber-pornography offenses requires a holistic and multidisciplinary approach. Continuous evaluation and refinement of regulations, capacity building of law enforcement agencies, and close international cooperation are essential steps to be taken. An effective strategy must consider not only law enforcement aspects but also prevention and rehabilitation, as well as involve various stakeholders to create a safer and more conducive digital ecosystem. With the right approach, it is hoped that law enforcement against cyber-pornography offenses can be carried out effectively and provide a significant deterrent effect while at the same time protecting the public, especially vulnerable groups, from the destructive impact of these crimes.

C. Strategies of the North Sumatra Regional Police in Combating Cyber-Pornography Offenses

In facing the increasingly alarming complexity of cyber-pornography offenses, the North Sumatra Regional Police has implemented a series of comprehensive strategies encompassing preventive, repressive, and rehabilitative aspects. This holistic approach is based on a deep understanding that cyber-pornography offenses involve not only technical and legal aspects but also the

psychological dimensions of perpetrators and victims, as well as their broad implications for the social fabric. As the vanguard of law enforcement in the North Sumatra region, the North Sumatra Regional Police is responsible for creating a secure and conducive digital ecosystem for the public, explicitly focusing on combating cyber-pornography offenses.

As a cornerstone of its countermeasure strategy, the North Sumatra Regional Police prioritizes the capacity building of cyber investigators through intensive and continuous training programs. These programs are comprehensively designed to equip investigators with the latest knowledge and skills in cybercrime and digital forensics. The training curriculum covers effective digital investigation techniques, comprehensive analysis of electronic evidence, and an in-depth understanding of relevant regulations, such as Law Number 11 of 2008 and Law Number 44 of 2008. In addition, investigators are also equipped with an understanding of digital rights and personal data protection, which are crucial in handling cybercrime cases in this modern era (Soemitro et al., 2023). With this enhanced capacity, investigators are expected to act more proactively and effectively in anticipating the modus operandi of perpetrators.

Complementing the strengthening of investigators' capacity, the North Sumatra Regional Police also invests significantly in procuring and utilizing advanced digital forensic technology. Specialized digital forensic software and hardware are optimally utilized to extract, recover, and analyze data from various electronic devices, such as smartphones, computers, and servers. This technology is vital in uncovering digital evidence that is hidden, encrypted, or even deleted by perpetrators, who often use various methods to conceal their criminal traces. Through this technology, it is expected that the process of proving cases in court will be more substantial and irrefutable, which in turn can deter perpetrators.

Recognizing that combating cyber-pornography offenses requires the active participation of all elements of society, the North Sumatra Regional Police proactively initiates and implements extensive digital literacy and education programs. These programs are designed to raise public awareness regarding the dangers of cyber-pornography and the urgency of cybersecurity. This education reaches various levels of society, from students at various levels of education to university students and parents, with materials specifically tailored to each group's needs and level of understanding. Through various communication channels, such as direct outreach, seminars, and creative public campaigns, the public is educated on safe internet practices, recognizing illegal content, and effective reporting mechanisms to the authorities. It is hoped that with increased digital literacy, the public can be more vigilant and protect themselves from these crimes.

Furthermore, the North Sumatra Regional Police also recognizes the importance of building strategic partnerships with internet service providers (ISPs) and social media platforms (Sihombing et al., 2024). Close collaboration with these stakeholders is key to breaking the chain of distribution of cyber-pornographic content. This partnership is realized by exchanging relevant information and data for investigation and law enforcement purposes while upholding the principles of data protection and privacy. Through a strong synergy between law enforcement agencies and digital service providers, it is hoped that identifying, blocking, and removing illegal content can be carried out more quickly and effectively, thereby minimizing the negative impacts. This cooperation also strengthens preventive efforts, as platforms can be more proactive in detecting and removing content that violates regulations.

As a form of long-term commitment, the North Sumatra Regional Police regularly evaluates and updates internal regulations related to handling cybercrimes. This process is crucial to ensure that existing regulations remain relevant and adaptive to technological developments and the ever-evolving modus operandi of perpetrators. In this evaluation process, the North Sumatra Regional Police also actively involve and consider input from various parties, including academics, legal practitioners, and civil society, to formulate comprehensive and effective regulations. It is hoped that these regulatory updates will provide an even stronger legal basis for law enforcement agencies in carrying out their duties while also providing a maximum deterrent effect on perpetrators of cyber-pornography offenses. Up-to-date and relevant regulations also support the creation of a safer and healthier digital ecosystem.

By implementing these comprehensive and sustainable strategies, the North Sumatra Regional Police endeavors not only to prosecute perpetrators of cyber-pornography offenses but also to build a safer and healthier digital ecosystem in North Sumatra. This holistic approach, which combines internal capacity building, utilization of advanced technology, community involvement, and cross-sectoral cooperation, is expected to have a significant long-term impact. Thus, it is hoped that the rate of cyber-pornography offenses can be reduced, and the public can be protected from the destructive impact of these crimes, and a more conducive and dignified digital space can be created for all citizens of North Sumatra. The strategies implemented also consider psychological aspects, both from the perspective of the perpetrator and the victim, to ensure a more effective and humane approach.

CONCLUSIONS AND SUGGESTIONS

Based on the findings and discussion, it can be concluded that cyber-pornography offenses in North Sumatra represent a complex and multidimensional phenomenon, demanding holistic, adaptive, and sustainable countermeasures. The North Sumatra Regional Police, as the leading law enforcement institution, plays a central role in combating these crimes in the digital era. Eradication efforts undertaken include mapping the anatomy of cyber-pornography offenses, encompassing the identification of patterns, modus operandi, targeted victims, and mediums used. The results of this mapping are crucial as a foundation for formulating effective countermeasure strategies. In practice, law enforcement against cyber-pornography offenses faces various significant challenges, ranging from the complexity of collecting and substantiating easily manipulated digital evidence, intricate issues of cross-border jurisdiction, the rapid pace of technological development that often surpasses the adaptive capacity of regulations and law enforcement agencies, to the limited capacity of human resources in the field of cyber law enforcement.

Nevertheless, the North Sumatra Regional Police has implemented a series of comprehensive strategies, including strengthening the capacity of cyber investigators through specialized training, utilizing cutting-edge digital forensic technology, promoting digital literacy and education programs to the broader community, building close collaboration with internet service providers and social media platforms, and continuously updating internal regulations. Despite this, synergy among stakeholders and the active participation of all elements of society remain determining factors in creating a secure, conducive, and dignified digital ecosystem in North Sumatra. Although showing positive results, these efforts must be continuously evaluated and refined to remain relevant and effective in facing the ever-evolving dynamics of cybercrime.

Based on the above conclusions, several strategic steps are recommended to enhance the effectiveness of combating cyber-pornography offenses in North Sumatra. *First*, there needs to be a significant increase in investment in state-of-the-art digital forensic technology, accompanied by continuous and comprehensive training programs for cyber investigators to keep pace with technological developments and perpetrators' modus operandi. *Second*, strengthening cooperation and coordination among law enforcement agencies at the national and international levels is imperative to overcome jurisdictional obstacles and expedite law enforcement processes, especially in cases involving perpetrators or digital platforms abroad. *Third*, digital literacy and education campaigns need to be promoted more massively, creatively, and targeted, involving the active participation of educational institutions, community organizations, influential figures, and the mass media to build collective awareness

and societal resilience against cyber-pornography. *Fourth*, it is essential to conduct in-depth studies and regulatory updates to be more specific and adaptive to technological advancements, including more explicitly regulating the responsibilities and obligations of social media platforms and internet service providers operating in Indonesia while upholding human rights principles and responsible freedom of expression. *Fifth*, there is a need to initiate comprehensive research and development periodically to map the factors influencing criminal behavior and understand the specific needs of victims with a perspective oriented to these factors to formulate more effective and humane intervention policies and strategies. Through the implementation of these recommendations, it is expected that the role of the North Sumatra Regional Police in combating cyber-pornography in the digital era can be further optimized, thus providing maximum protection for the public and creating a safer, healthier, and more dignified digital space.

REFERENCES

Agustini, S., Tan, W., & Geovanni, G. (2023). Analisis Hukum Terhadap Penyampaian Informasi Elektronik yang Melanggar Norma Moral. *Ajudikasi: Jurnal Ilmu Hukum, 7*(2), 349-374. https://doi.org/10.30656/ajudikasi.v7i2.7665

Boopathi, S., & Sneka, E. (2024). Cyber Law and the Dark Web: Regulating Hidden Markets. *Journal of Law and Legal Research Development, 1*(4), 17-24. https://doi.org/10.69662/jllrd.v1i4.28

Handoyo, B., Husamuddin, M. Z., Rahma, I., & Asy'ari, A. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *Maqasidi: Jurnal Syariah dan Hukum, 4*(1), 40-55. https://doi.org/10.47498/maqasidi.v4i1.2966

Husen, L. O., Salle, S., Syalman, A. A., & Muzakkir, A. K. (2020). Pengamanan Intelijen Kepolisian Terhadap Putusan Pengadilan Atas Objek Sengketa. *SIGn Jurnal Hukum, 1*(2), 136-148. https://doi.org/10.37276/sjh.v1i2.62

Irwansyah. (2021). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel* (Revision Edition). Mirra Buana Media.

Latifansyah, M. A., Rifai, A., & Sadino, S. (2024). Legal Measures to Support the Process of Asset Recovery in the State-Owned Enterprises Banking Sector Post-Corruption Cases. *Al-Ishlah: Jurnal Ilmiah Hukum, 27*(2), 427-452. https://doi.org/10.56087/aijih.v27i2.514

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/138

Law of the Republic of Indonesia Number 44 of 2008 on Pornography (State Gazette of the Republic of Indonesia of 2008 Number 181, Supplement to the State Gazette of the Republic of Indonesia Number 4928). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/171

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/1683

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://jdih.dpr.go.id/setjen/detail-dokumen/tipe/uu/id/1842

Nasrullah, N. (2023). Implementing Chemical Castration Punishment: A Perspective on Criminal Law and Human Rights. *SIGn Jurnal Hukum, 4*(2), 402-413. https://doi.org/10.37276/sjh.v4i2.282

Nugroho, A. W., Rabbani, A. A., & Ristoka, A. T. (2024). Analisis Kriminologi Kasus Kristen Gray: Pelanggaran Peraturan Pandemi dan Penyalahgunaan Izin Tinggal Keimigrasian di Indonesia. *Jurnal Ilmiah Universitas Batanghari Jambi, 24*(1), 166-175. https://doi.org/10.33087/jiubj.v24i1.4659

O'Malley, R. L., & Holt, K. M. (2022). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence, 37*(1-2), 258-283. https://doi.org/10.1177/0886260520909186

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum, 4*(2), 320-331. https://doi.org/10.37276/sjh.v4i2.252

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn).

Rivanie, S. S., Komuna, A. P., Putra, A. A., Utama, P. F., & Muzakkir, A. K. (2021). Protection of Children as Perpetrators of Criminal Act Stimulated by Pornography Based on Indonesian Laws. *Musamus Law Review, 4*(1), 1-15. https://doi.org/10.35724/mularev.v4i1.3759

Salsabilla, S., Razif, I. B., & Albab, U. (2023). Legal Protection against Sexual Violence on Women: A Study on Legislation. *SIGn Jurnal Hukum, 5*(2), 249-262. https://doi.org/10.37276/sjh.v5i2.288

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Sihombing, R. P., Kusno, K., & Siregar, A. A. (2024). Investigative Effectiveness in the Digital Era: A Case Study of Technological Innovation at the Rokan Hilir Police Resort. *SIGn Jurnal Hukum, 6*(2), 52-67. https://doi.org/10.37276/sjh.v6i2.368

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum, 5*(1), 155-167. https://doi.org/10.37276/sjh.v5i1.272

Suhyana, F. A., Suseno, S., & Ramli, T. S. (2021). Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain. *SIGn Jurnal Hukum, 2*(2), 138-156. https://doi.org/10.37276/sjh.v2i2.92

Tombolotutu, R. N. F., Chandra, T. Y., & Mau, H. A. (2024). Proving Illegal Access in Combating Cybercrime in Indonesia. *Journal of Law and Regulation Governance, 2*(8), 260-271. https://doi.org/10.57185/jlarg.v2i8.59

Zaltina, P., & Nurtjahyo, L. I. (2024). Right to be Forgotten as a Legal Protection for the Victims of Electronic Sexual Violence Cases. *The Indonesian Journal of Socio-Legal Studies, 3*(2), 1-30. https://doi.org/10.54828/ijsls.2024v3n2.4