



# CRIMINOLOGICAL ANALYSIS OF EFFORTS TO COUNTER SEXTORTION THROUGH ELECTRONIC MEDIA

Muhammad Al Ghifary Hasbani<sup>1\*</sup>, Dona Raisa Monica<sup>2</sup>, Fristia Berdian Tamza<sup>3</sup>, Deni Achmad

*Faculty of Law, University of Lampung<sup>1,2,3,4</sup>*

[alghyfhari.hs@gmail.com](mailto:alghyfhari.hs@gmail.com)<sup>1</sup>, [dona.raisa@fh.unila.ac.id](mailto:dona.raisa@fh.unila.ac.id)<sup>2</sup>, [fristia.berdian@fh.unila.ac.id](mailto:fristia.berdian@fh.unila.ac.id)<sup>3</sup>,

[deni.achmad@fh.unila.ac.id](mailto:deni.achmad@fh.unila.ac.id)<sup>4</sup>

## Abstract

This study aims to analyze sextortion, a form of sexual extortion conducted through electronic media, from a criminological perspective by identifying the motives and behavioral patterns of offenders, the characteristics of victims, and evaluating the effectiveness of law enforcement efforts in addressing this type of cybercrime in Indonesia. This study employs a descriptive juridical-normative method, utilizing historical data, previous studies, and literature reviews from relevant academic journals and scientific publications. The analysis focuses on applicable legal regulations, legal doctrines, and various sextortion cases that occurred in Indonesia between 2021 and 2024. The findings indicate that sextortion is not merely a criminal act of extortion but also involves psychological manipulation, sexual exploitation, and digital victimization, while revealing a significant gap between the rapid development of cybercrime methods and the capacity of law enforcement authorities, particularly in handling digital evidence and cross-border jurisdictions. This study is limited by its qualitative scope and focus on the Indonesian legal system, which may not fully represent the dynamics of sextortion at the global level. Nevertheless, it contributes to the development of studies in criminology, cyber law, and victimology by presenting an interdisciplinary analysis that enriches academic understanding and offers practical recommendations for policymakers and law enforcement agencies to formulate more effective legal and preventive measures. The novelty of this study lies in the integration of criminological and descriptive juridical-normative approaches to conceptualize sextortion as a multidimensional cybercrime phenomenon in Indonesia, emphasizing the importance of reforming cybercriminal law to align with technological advancements and contemporary social challenges.

**Keywords:** *Sextortion, criminology, sexual extortion, cybercrime, cyber law, victimology, law enforcement.*

## 1. Introduction

The development of information and communication technology over the past two decades has fundamentally changed how humans interact, work, and build social relationships. The internet, initially designed as a medium for information exchange, has evolved into a complex social space where the boundaries between the real and virtual worlds are increasingly blurred. According to We Are Social (2024), the number of internet users in Indonesia has reached approximately 221 million people, or about 80% of the total population, with more than 170 million active social media users daily (source: [apjii.or.id](http://apjii.or.id)). While the accessibility of information and digital interaction has provided significant benefits for economic and educational development, it has also given rise to new forms of cybercrime, one of which is sexual extortion through electronic media. Sextortion is a term derived from the combination of sex and extortion, which broadly refers to coercing someone to provide money, sexual services, or personal content under the threat of disseminating sexual or pornographic material of the victim (Ratnasari et al., 2025).

This occurs when perpetrators obtain victims' images, videos, or personal information—either through online relationships, hacking, or emotional manipulation—and use them as tools for blackmail. This phenomenon has been on the rise in Indonesia, alongside the growing use of social media and instant messaging platforms. According to SAFEnet's 2023 report, there were 1,052 complaints related to Online Gender-Based Violence (OGBV) in Indonesia, of which approximately 12.64% were cases of sextortion (Source: [tirto.id](http://tirto.id)). Indonesia is among the top five Southeast Asian countries with the highest rates of sextortion, with increasingly diverse methods and cross-border criminal networks (source: [ti.or.id](http://ti.or.id)).



The phenomenon of sextortion should not be viewed merely as a moral or ethical violation in digital communication but as a criminal offense under Indonesian law, particularly those related to extortion (Articles 368 and 369 of the Criminal Code), pornography (Law No. 44 of 2008), and misuse of electronic information (Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions). However, law enforcement against sextortion cases still faces numerous challenges, such as difficulties in proving criminal elements, limited digital forensic capabilities, and insufficient victim protection. From a criminological perspective, sextortion represents not only an economic crime but also psychological and sexual exploitation, where perpetrators exploit victims' emotional and social vulnerabilities to achieve their goals.

This crime results not only in material losses but also severe psychological trauma, and in some cases, has led victims to suicide due to social pressure and shame. Several studies have explored the phenomenon of sextortion from various perspectives; however, most remain focused on positive legal frameworks without deeply integrating criminological approaches to it. Kadir (2025) argues that sextortion represents a new form of digital sexual violence that emerges from power imbalances in cyberspace. Tatang (2025) noted that the enforcement of sexual crime laws continues to face significant obstacles. Meanwhile, Arafat and Wirasto (2024) emphasized the importance of digital forensic capabilities in handling sextortion cases across Southeast Asia. They found that most law enforcement agencies in the region still struggle with resource and technical limitations in tracking cross-border offenders. However, these studies have not proposed specific legal policy directions tailored to the Indonesian context.

These studies indicate a research gap in the holistic understanding of sextortion in Indonesia. Most prior research has focused on normative legal aspects, while the criminological and sociological dimensions of offender behavior and victim characteristics remain underexplored. Furthermore, debates continue regarding the legal status of sextortion within Indonesia's legal system, as no specific legislation explicitly defines it as a distinct criminal offense. This legal ambiguity poses challenges to the application of criminal provisions and potentially undermines the effectiveness of law enforcement.

The urgency of this study is driven by the rising number of sextortion cases, which significantly impact social order and public morality. In the context of criminal law enforcement, a gap remains between the social realities of cybercrime and the capacity of positive law to anticipate and prosecute offenders. Therefore, the main objective of this research is to analyze the phenomenon of sextortion from a criminological perspective, examining offenders' motives, behavioral patterns, victim characteristics, and the effectiveness of law enforcement in Indonesia. This study also highlights the importance of legal and policy reforms that align with technological developments and the social challenges faced by digital communities.

Theoretically, this study contributes to the advancement of criminal law and cyber criminology by offering an interdisciplinary approach that integrates juridical-normative analysis with behavioral studies. Practically, the findings are expected to provide insights for policymakers and law enforcement agencies in formulating strategic measures for the prevention, prosecution, and victim protection in sextortion cases in Indonesia. Thus, this study is not only academically relevant but also holds significant practical value in strengthening the national legal system amid the complexities and vulnerabilities of the digital age.

## **2. Literature review and hypothesis/es development**

The rapid advancement of information and communication technology over the past two decades has drastically transformed human interaction and engagement in daily activities. The increasingly open digital world has brought immense benefits in social, economic, and educational aspects, yet at the same time, it has also given rise to new and complex forms of crime (Sukma et al., 2025). One emerging phenomenon in the realm of cybercrime is sextortion, which refers to acts of extortion and threats using sexually explicit content via electronic media. This phenomenon is particularly alarming, as it involves the exploitation of human dignity through technological means, causing victims to suffer not only financial loss but also deep psychological and social distress. Sextortion is a modern crime rooted in



psychological manipulation, power, and technology, which is fundamentally different from traditional extortion (Putri & Sukmareni, 2024).

Within the Indonesian criminal law system, sextortion has not yet been explicitly regulated as a distinct criminal offense. However, several legal provisions can serve as the foundation for prosecuting offenders. For instance, Articles 368 and 369 of the Criminal Code (KUHP) address extortion and threats, while Articles 27(1) and 29 of Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law) prohibit the distribution or threat of distributing obscene content. Additionally, Article 4 of Law No. 44 of 2008 on Pornography explicitly forbids the creation and dissemination of pornographic material. Nevertheless, the application of these provisions often encounters obstacles, primarily due to the absence of a clear legal category that specifically accommodates sextortion as a cyber-based sexual crime. Consequently, law enforcement officers frequently face challenges in proving the interrelated elements of sexuality and digitalization as components of a single criminal act. This legal gap underscores the urgent need for legislative reform that is more adaptive to social realities and technological developments that underlie the emergence of new forms of crime.

Sextortion should not only be viewed as an economic crime intended for financial gain, but also as a power-based sexual crime. Perpetrators often exploit emotional connections, trust, or the vulnerability of their victims to gain control. According to the Rational Choice Theory proposed by Clarke and Cornish (1985), individuals commit crimes based on rational assessments of potential risks and rewards. In the digital context, anonymity and ease of accessing personal information provide opportunities for offenders to commit crimes with relatively low risk (Gunawan, 2025). Meanwhile, Agnew's (1992) Strain Theory explains that social pressure, economic frustration, or unmet psychological needs can push individuals to engage in illegal behavior to achieve their goals.

Thus, sextortion can be understood as the result of an interaction between personal motives and opportunities afforded by technology. From a victimological perspective, victims of sextortion are generally individuals with low digital literacy and a high tendency to trust online interactions (Adiarti & Fadhilah, 2025). They are often unaware of the risks associated with sharing personal information or intimate content online. After becoming victims, many are reluctant to report their experiences because of shame, fear of social stigma, or anxiety about the potential dissemination of their personal content (Maulida & Romdoni, 2024). This situation exacerbates victims' suffering and leads to revictimisation, in which victims experience further harm through legal processes, media coverage, or unsympathetic social treatment. From a criminological standpoint, this reflects the weaknesses in the legal protection system for victims of cybercrimes, particularly those involving sexuality and personal privacy.

Previous studies have provided valuable insights into the phenomenon of sextortion from different perspectives. Yungsiana and Prabandari (2024) describe sextortion as a form of digital sexual exploitation that combines emotional manipulation and psychological coercion. They emphasize the importance of understanding the power dynamics underlying such acts, where technology serves as an instrument of domination. However, their study focuses mainly on Western contexts and does not examine legal dynamics in Southeast Asia. Yudhistira and Puspitosari (2025) argue that current regulations remain too general and fail to address the complexity of digital crimes involving moral and sexual elements.

Meanwhile, Najwa (2024) highlights the difficulties faced by law enforcement agencies in Southeast Asia in handling cross-border sextortion cases because of limited forensic technology and inadequate international cooperation in cyber law enforcement. From these studies, it becomes evident that the main challenges in addressing sextortion lie not only in substantive legal aspects but also in law enforcement capacity and in victim protection. Prior research tends to focus primarily on normative legal dimensions without delving deeply into the criminological factors that drive offender behavior and victim vulnerability. Therefore, an interdisciplinary approach that combines juridical-normative analysis with criminological and victimological perspectives is essential for gaining a more comprehensive understanding of sextortion in Indonesia.



A review of the literature reveals that sextortion has evolved from a form of extortion into a distinct type of digital sexual crime, characterized by the convergence of extortion, sexual exploitation, and technological misuse. This complexity calls for the reconceptualization of existing legal norms, enabling law enforcement to adapt to the realities of crime in the digital era. However, weak regulations and limited capacity among law enforcement officers in handling electronic evidence have created a gap between written law and its practical implementation. This highlights the urgent need for criminal law reform that not only emphasizes offender punishment but also strengthens prevention, digital literacy, and victim protection. In conclusion, this study asserts that sextortion must be understood as a multidimensional socio-legal phenomenon. On the one hand, it challenges the effectiveness of positive law in prosecuting offenders; on the other hand, it underscores the necessity of reforming criminal law to accommodate changes in human behavior in the digital age. Integrating criminological perspectives with juridical-normative analysis is expected to serve as a foundation for developing adaptive, humanistic, and responsive legal policies to address Indonesia's evolving cybercrime landscape.

### **3. Methodology**

This study employs a descriptive juridical (normative juridical) method, focusing on the analysis of positive law and its application to the phenomenon of sextortion as a form of cybercrime in Indonesia (Saebani 2021). This approach involves examining applicable legal materials, legal theories, academic literature, and relevant previous research to systematically describe and explain the relationship between legal norms and the social realities of cybercrime. The data used in this research are derived from primary legal materials, namely statutory regulations such as the Criminal Code (KUHP), Law Number 19 of 2016 concerning Electronic Information and Transactions, and Law Number 44 of 2008 concerning Pornography; secondary legal materials, including books, journals, reports from law enforcement agencies, and international publications; and tertiary legal materials, such as legal dictionaries and encyclopedias.

Data collection was conducted through library research to obtain valid and academically verified information. The data were then analyzed using a descriptive qualitative method by interpreting and comparing existing legal norms with the sextortion phenomenon that occurs in society. This analysis aims to identify the alignment between legal norms and law enforcement practices, as well as to assess the extent to which the national legal system can effectively respond to digital sexual extortion crimes. The scope of this study is limited to the discussion of criminal law and criminology within the context of Indonesia's positive law, without involving any field research. The results of this analysis are expected to provide both academic and practical contributions to the development of cybercriminal law, particularly in the formulation of legal policies that are more adaptive, humanistic, and responsive to the phenomenon of sextortion in the digital era.

### **4. Results and discussion**

The findings of this study indicate that the phenomenon of sextortion in Indonesia represents a highly complex and multidimensional form of cybercrime involving a combination of elements such as extortion, sexual exploitation, digital threats, and the misuse of information technology. An analysis of positive law reveals that this criminal act has not yet been explicitly regulated within Indonesia's criminal justice system; however, its constituent elements are implicitly contained within several statutory provisions. Acts in which offenders threaten victims with the dissemination of intimate photos or videos to obtain financial gain, sexual favors, or other forms of compliance may be prosecuted under Article 368 of the Criminal Code (KUHP) on extortion, Article 369 of the KUHP on threats, and Articles 27(1) and 29 of Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law), which prohibits the distribution and threats of dissemination of obscene content. If the offender's actions involve the creation, storage, or distribution of pornographic material, Articles 4 and 6 of Law No. 44 of 2008 on Pornography may apply. Nevertheless, this legal framework remains sectoral and fragmented, often resulting in overlapping norms in law enforcement, particularly when investigators face cases involving complex digital evidence and anonymous perpetrators.

In practice, law enforcement authorities face numerous challenges in classifying sextortion as a criminal offense. The absence of explicit regulations defining sextortion leads to interpretative disparities among



investigators, prosecutors, and judges during legal proceedings. One of the primary challenges is proving mens rea (criminal intent) and the direct connection between threats and sexual elements in the content. In many cases, perpetrators claim that their relationship with the victim was consensual or that the shared content was a matter of mutual agreement. Such arguments blur the boundaries between privacy and criminality and weaken victims' positions before the law. Many victims also refrain from reporting these crimes because of fear of social stigma, shame, or further exposure of their intimate content. This phenomenon reveals both legal and social asymmetry, exacerbating victims' suffering and demonstrating the weakness of legal protection mechanisms for victims of cyber-based sexual crime.

From a criminological perspective, sextortion is a crime rooted in power relations and psychological domination between the perpetrator and victim. Offenders exploit victims' emotional connections, trust, or vulnerabilities to exert control and engage in sexual exploitation. According to the Rational Choice Theory (Clarke & Cornish, 1985), offenders act rationally by weighing the risks and benefits of their actions. The digital environment offers vast opportunities for offenders because of the relatively low risk of detection compared to the high potential for financial and psychological rewards. Moreover, anonymity in cyberspace provides offenders with a sense of protection, allowing them to operate without revealing their identities. In some cases, offenders operate in groups, forming organized transnational criminal networks that use social media, the dark web, or encrypted applications to extort victims through online scams. According to Interpol (2023), Indonesia ranks among the top five Southeast Asian countries experiencing an increase in cross-border sextortion cases, with most perpetrators operating in the Philippines and Nigeria. Victims are typically teenagers and young adults who are active social media users.

From a victimological standpoint, the characteristics of sextortion victims in Indonesia are generally similar. The majority are between 15 and 25 years old, have low digital literacy, and are intensive social media users. Many victims are unaware of digital privacy risks and easily trust the online identities presented by perpetrators. In many cases, offenders use digital grooming techniques, gradually building the victim's trust through emotional or romantic approaches until the victim willingly shares personal information. Once this trust is established, perpetrators exploit the situation to issue threats and extort their victims. This pattern indicates that sextortion is not merely a crime against property or the body but also against the mind, dignity, and personal freedom of victims. The psychological impacts are profound, including shame, trauma, depression, and, in some cases, suicide. This phenomenon underscores that sextortion is a form of sexual violence based on psychological control, inseparable from the socio-cultural context in Indonesia, where issues of sexuality are often regarded as taboo.

Another major obstacle in law enforcement is the limited digital forensic capacity of law enforcement agencies and a lack of cross-jurisdictional cooperation. Many offenders utilize foreign servers or social media platforms that operate outside Indonesia's legal jurisdiction, such as Facebook, Instagram, Telegram and WhatsApp. Consequently, law enforcement authorities must rely on international cooperation mechanisms, such as Mutual Legal Assistance (MLA), to obtain data and electronic evidence from other countries, a process that is often time-consuming and not always successful. According to a Bareskrim Polri (2023) report, approximately 65% of reported sextortion cases in Indonesia involve anonymous perpetrators who cannot be traced because of the use of fake accounts and digital masking tools such as VPNs or fake IP addresses. These technical challenges highlight the urgent need to enhance law enforcement capacity in information technology and establish a specialized coordinating body to handle technology-based sexual crimes in an integrated way.

In addition to technical constraints, social and cultural factors hinder effective handling of sextortion cases. The strong patriarchal culture and conservative attitudes toward sexuality often prevent victims from reporting incidents because of fear of blame or humiliation. The social stigma surrounding victims of digital sexual violence remains high; victims are frequently perceived as complicit because they "shared" their intimate content. This further marginalizes victims and impedes justice, as law enforcement officers sometimes carry moral or cultural biases in their work. This condition demonstrates the need for a paradigm shift within both the legal system and society, viewing digital



sexual violence not from a moralistic standpoint but as a violation of human rights and an offense against personal integrity.

Based on the literature review and legal analysis, it can be concluded that Indonesia's legal system remains reactive and insufficiently adaptive to the evolving nature of technology-based sexual crimes. Law enforcement remains focused on formal criminal aspects, often overlooking the social and psychological dimensions of victimization. In many cases, victims experience revictimisation during legal proceedings due to humiliating questioning or unrealistic evidentiary demands. Crimes such as sextortion require a more victim-sensitive legal approach grounded in human rights protection principles. The state must act not only as an enforcer of justice but also as a protector and restorer of victims through empathetic and humanistic policies.

The findings further indicate the urgent need for criminal law reform to align with the evolving landscape of cybercrimes in the digital era. This reform should include the establishment of specific legal provisions defining sextortion as a distinct criminal offense, with characteristics and penalties that differ from those of conventional extortion. Such provisions must encompass digital, sexual, and psychological dimensions of abuse. Additionally, strengthening law enforcement capacity through training in digital forensics, cyber investigation techniques, and gender-sensitive handling of digital sexual violence cases is essential. The government must also enhance international cooperation for data sharing, cross-border tracking, and the prosecution of offenders operating beyond national jurisdictions.

However, preventive and educational measures must complement law enforcement efforts. The government, in collaboration with educational institutions, the media, and civil society organizations, should promote digital and legal literacy, particularly among young people who are most vulnerable to victimization. Education on digital safety, online privacy, and the risks of sharing personal content should be implemented systematically. Moreover, formulating ethical guidelines for social media use, emphasizing legal awareness and respect for others' privacy, is crucial to prevent risky behaviors in digital spaces.

Overall, the findings and discussion demonstrate that sextortion in Indonesia is not only a legal challenge but also a social, technological, and moral challenge. This crime reflects the transformation of criminal behavior in the digital era, where technology serves as an instrument of power and control, capable of destroying a person's life without physical contact. Therefore, the national legal system must evolve accordingly to strengthen victim protection and ensure comprehensive justice. The law must not only punish offenders but also create a sense of digital security within society. Through an integrated approach combining legal, criminological, and social-educational aspects, Indonesia can build a more responsive and resilient legal system capable of addressing cybercrimes, particularly sextortion, and protecting its citizens from sexual exploitation in an ever-evolving technological age.

## **5. Conclusion**

### **5.1. Conclusion**

Based on the results of the research and analysis conducted, it can be concluded that the phenomenon of sextortion represents a form of cybercrime with complex legal, social and psychological dimensions. The objective of this study—to analyze sextortion from legal and criminological perspectives— was achieved by illustrating the relationship between technological development and the emergence of new forms of digital sexual extortion in Indonesia. The analysis shows that acts of sextortion essentially fulfill the elements of extortion as stipulated in Articles 368 and 369 of the Indonesian Criminal Code (KUHP), as well as the elements of threats and indecency violations as regulated in Articles 27(1) and 29 of the Electronic Information and Transactions Law (Law No. 19 of 2016) and the Pornography Law (Law No. 44 of 2008). Nevertheless, the existing legal framework remains insufficiently specific to address technology-based sexual crimes, which possess distinct characteristics and modes of operation compared to conventional extortion crimes. Therefore, there is an urgent need for cybercriminal law reform to accommodate the evolving forms of crimes involving sexual exploitation in digital spaces.



From a criminological perspective, this study demonstrates that sextortion is not merely an act of extortion but also a form of sexual violence rooted in the abuse of power, psychological manipulation and digital domination. Offenders exploit victims' emotional vulnerabilities through online grooming or identity deception to gain control of their behavior. From the victims' perspective, the study reveals that young women and adolescents are the most vulnerable groups because of low levels of digital literacy and the strong social stigma surrounding sexuality. Victims often experience severe psychological distress and are reluctant to report incidents for fear of the spread of their private content and societal stigma. These findings highlight the importance of adopting a more humanistic and victim-centered approach to enforcing laws against sextortion, ensuring that victims do not experience revictimization during the legal process. In conclusion, this study successfully achieved its primary goal of identifying the gap between legal norms, the dynamics of cybercrime, and victim protection in the context of sextortion in Indonesia.

### **5.2. Limitation**

This study has several limitations that must be acknowledged to ensure that the findings are interpreted proportionally. First, the study employs a descriptive juridical (normative juridical) approach, focusing on the analysis of legal norms and academic literature; thus, it does not include field data or interviews with law enforcement officials or sextortion victims. Consequently, this study cannot empirically illustrate the actual dynamics of law enforcement at the investigative or judicial levels.

Second, owing to its qualitative and literature-based nature, this study relies primarily on secondary data obtained from journals, institutional reports, and official publications. Consequently, there is a possibility that the data used may not fully reflect the most recent conditions of sextortion cases in Indonesia, particularly those occurring at the local level or within small online communities. Furthermore, this study mainly emphasizes criminal law and criminological aspects, without exploring the psychological dimensions and digital forensic technologies, which are also highly relevant to the handling of sextortion cases. The author recognizes that an interdisciplinary study involving experts in psychology, sociology, and information technology would yield more comprehensive and applicable results. However, owing to the conceptual and literature-based scope of this research, the discussion has been primarily directed toward normative and analytical dimensions.

Another limitation is the lack of consistent statistical data on sextortion cases in Indonesia, as many victims choose not to report incidents, resulting in the dark number of crime phenomena. Therefore, the findings of this study are more interpretative and conceptual. Nonetheless, they are expected to serve as a foundation for future empirical research that further explores the legal, social, and psychological dynamics of sextortion in Indonesia.

### **5.3. Suggestion**

Based on the findings and limitations outlined above, several recommendations can be proposed as references for addressing sextortion in Indonesia. First, it is essential to undertake a comprehensive reform of national criminal law by explicitly recognizing sextortion as a specific criminal offense within the Electronic Information and Transactions Law (ITE Law) or through an amendment to the Criminal Code (KUHP). This reform would provide a clear and unambiguous legal foundation that prevents multiple interpretations. The regulation should include a precise definition, elements of the offense, and penalties that consider both the digital dimension and the psychological impact on the victims.

Second, enhancing the capacity of law enforcement officers is crucial, particularly in the areas of digital forensics, cyber investigation techniques and empathetic approaches to victims of digital sexual violence. Cross-sectoral training programs are necessary to ensure that law enforcement practices are professional, technically competent, and victim centered. Third, the government should strengthen international cooperation with global institutions such as Interpol and the ASEAN Cybercrime Center to accelerate the tracking of cross-border offenders and reinforce the Mutual Legal Assistance (MLA) framework.



Fourth, public education and digital literacy programs should be promoted from an early age to raise awareness of personal data security and the dangers of digital manipulation. Schools, media, and civil society organizations must play active roles in cultivating responsible and safe online behavior. Finally, a comprehensive victim protection and rehabilitation mechanism should be developed, including accessible psychological counseling and legal assistance services. These measures are expected to enable Indonesia's legal system to respond to sextortion more effectively, justly, and in alignment with human rights protection principles in this digital era.

## References

### Books

- Agnew, R., & Brezina, T. (2019). General strain theory. In *Handbook on crime and deviance* (pp. 145–160). Cham: Springer International Publishing.
- Archer, M., & Tritter, J. (2000). Rational choice theory: Resisting colonization.
- Gunawan, R. (2025). Patterns of social media use and the risk of victimization. *Buatbuku.com*.
- Saebani, B. A. (2021). *Legal research methods: A juridical-normative approach*.
- Sukmana, O., Sulistyarningsih, T., Damanik, F. H. S., Wahyudi, F. D., Ras, A., Astari, F., ... & Fauziyah, N. K. (2025). *Digital sociology: Social transformation in the technological era*. Star Digital Publishing.

### Journal Articles

- Adiarti, D. I., & Fadhilah, N. (2025). Building digital resilience among rural youth: An analysis of digital sexual violence from child development and gender perspectives. *Journal of Social Sciences and Education*, 3(1), 6–17.
- Arafat, M., & Wirasto, A. T. E. (2024). Criminal policy in handling cybercrime in the digital era: A case study in Indonesia. *Equality: Journal of Law and Justice*, 1(2), 220–241.
- Kadir, Z. K. (2025). From privacy to exploitation: Mapping the criminalization of revenge porn in the social media era. *Dewantara: Journal of Social Humanities Education*, 4(1), 133–152.
- Maulida, G., & Romdoni, M. (2024). Legal protection for victims of sexual harassment who experience secondary victimization on social media. *Southeast Asian Journal of Victimology*, 2(1), 59–79.
- Najwa, F. R. (2024). Legal analysis of cyber security challenges: A case study of cyber law enforcement in Indonesia. *Al-Bahts: Journal of Social, Political, and Legal Studies*, 2(1), 8–16.
- Putri, K. A., & Sukmareni, S. (2024). Regulation of extortion crimes using pornographic photos or videos (sextortion): A gender-based cyber perspective in Indonesia's positive law. *Innovative: Journal of Social Science Research*, 4(5), 7505–7515.
- Ratnasari, D., Rompas, D. D., & Tuwaidan, H. F. (2025). Legal protection for victims of extortion in sexual video call cases under the ITE Law. *Lex Administratum*, 13(1).
- Tatang, T. (2025). Law enforcement against digital-based sexual violence crimes in Depok City: A study on the effectiveness of the implementation of the ITE Law and the new Criminal Code. *Impresi Indonesia Journal*, 4(8), 2865–2874.
- Yudhistira, F. A., & Puspitosari, H. (2025). Law enforcement against perpetrators of indecent and child pornography websites. *Lex Generalis Law Journal*, 6(7).
- Yungsiana, I., & Prabandari, Y. S. (2024). The psychological dynamics of sextortion victims: A literature review. *Indonesian Journal of Forensic Psychology*, 4(1).

### Websites

- Indonesian Internet Service Providers Association (APJII). (2024, February 7). *APJII: The number of internet users in Indonesia reaches 221 million*. Retrieved from <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Transparency International Indonesia. (2021). *Corruption called "sextortion"*. Retrieved from <https://ti.or.id/korupsi-bernama-sextortion/>



Article Author. (2024, December 27). *The suffering of sextortion victims amid the lack of protection*. Retrieved from <https://tirto.id/derita-korban-sextortion-di-tengah-minimnya-perlindungan-korban-g6ZC>