



Criminal Liability for Online Gender-Based Sextortion Against Women Under Indonesian Criminal Law

Tanggung Jawab Pidana Pelaku Sextortion Berbasis Gender Online terhadap Perempuan di Indonesia

Rafli H. Husain¹, Dian Ekawaty Ismail², Mohamad Rivaldi Moha³

¹⁻³Faculty of Law, Gorontalo State University, Indonesia

Article Info

Corresponding Author:

Rafli H. Husain

✉ husainrafli506@gmail.com

History:

Submitted: 25-04-2026

Revised: 25-05-2026

Accepted: 28-05-2026

Keyword:

Sui Generis Offense; Bodily Autonomy Protection; Secondary Victimization; Cyber-Extortion.

Kata Kunci:

Delik Sui Generis; Perlindungan Otonomi Tubuh; Viktimisasi Sekunder; Pemerasan Siber.

Abstract

The Indonesian criminal justice system currently faces a profound regulatory vacuum regarding online gender-based sextortion, relying on a deeply fragmented statutory framework that structurally fails to capture the offense's complex hybrid nature. To resolve this severe doctrinal crisis, this study utilized a purely normative legal methodology, strictly excluding empirical statistical data, to critically evaluate existing domestic penal instruments. The profound analysis explicitly reveals that forcing cyber-extortion into conventional property or generic morality statutes systematically institutionalizes secondary victimization against women. Consequently, this article argues that applying existing laws is substantively inadequate and inherently violates the fundamental principle of strict legal certainty. Eradicating this pervasive systemic disparity strictly requires the immediate legislative formulation of a sui generis, gender-responsive penal provision. By shifting the regulatory paradigm from property-centric doctrines to comprehensive bodily autonomy protection, this conceptual framework provides a vital prescriptive blueprint for global jurisdictions struggling against the asymmetric weaponization of digital intimacy.

Abstrak

Sistem peradilan pidana Indonesia saat ini menghadapi kekosongan regulasi mendalam terkait sextortion berbasis gender daring, karena bersandar pada kerangka regulasi terfragmentasi yang gagal menangkap sifat hibrida kompleks kejahatan tersebut. Guna menyelesaikan krisis doktrinal ini, penelitian ini telah menggunakan metodologi hukum normatif murni, dengan secara ketat meniadakan data statistik empiris, untuk mengevaluasi instrumen pidana domestik. Analisis kritis mengungkap bahwa pemaksaan kejahatan pemerasan siber ke dalam pasal harta benda konvensional atau kesusilaan umum secara sistematis melembagakan viktimisasi sekunder terhadap perempuan. Oleh karena itu, artikel ini berargumen bahwa penerapan aturan hukum yang ada sangat tidak memadai dan terbukti melanggar prinsip kepastian hukum secara substantif. Pemberantasan disparitas sistemik yang masif ini mutlak membutuhkan perumusan legislatif segera atas delik pidana *sui generis* yang berperspektif gender. Melalui pergeseran paradigma dari doktrin berbasis properti menuju perlindungan otonomi tubuh komprehensif, kerangka konseptual ini memberikan cetak biru preskriptif vital bagi yurisdiksi global yang melawan persenjataan asimetris atas intimasi digital.



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA).

doi: <https://doi.org/10.65101/lawric.v2i1.289>

A. INTRODUCTION

1. Background

The contemporary global legal landscape is currently grappling with a profound regulatory vacuum regarding the prosecution of online gender-based violence (OGBV), a crisis most acutely manifested in the phenomenon of sextortion. Rather than a mere technological iteration of traditional crimes, sextortion represents a highly complex hybrid offense that inextricably intertwines elements of sexual exploitation, digital coercion, and economic or relational extortion. In Indonesia, this phenomenon exposes a critical clash of norms (*clash of norms*) between the ideal constitutional mandate of the state to protect bodily autonomy and digital privacy (*das sollen*) and the empirical reality of a deeply fragmented statutory framework (*das sein*). Data indicates an alarming escalation of this offense; the National Commission on Violence Against Women (Komnas Perempuan) documented 1,801 digital gender-based violence victims in 2023, while SAFEnet reported 1,902 complaints in 2024, with women constituting the overwhelming majority of victims.¹ Furthermore, transnational surveys indicate that Indonesia suffers the highest prevalence of sextortion cases across 17 Asian nations, reaching a critical threshold of 18%. This disproportionate vulnerability positions the Indonesian jurisdiction as a vital locus for international legal scholars to examine the systemic failure of conventional criminal law to adapt to the weaponization of intimate digital data.

Despite the escalating prevalence and severity of sextortion, the Indonesian criminal justice system lacks a *sui generis* statutory provision specifically criminalizing this behavior. Consequently, prosecutorial mechanisms are compelled to rely on a patchwork of partial, overlapping, and often contradictory regulations. Currently, law enforcement arbitrarily navigates between the Indonesian Criminal Code (KUHP) concerning conventional extortion, Law Number 1 of 2024 on Electronic Information and Transactions (ITE Law), Law Number 44 of 2008 on Pornography, and Law Number 12 of 2022 on Sexual Violence Crimes (TPKS Law).² This regulatory fragmentation epitomizes a systemic delay in legal responsiveness. Each of these statutes was enacted with

¹ Combine Resource Institution, "Hari Perempuan Internasional 2025: Menyuarakan Kerentanan Dan Kekerasan Berbasis Gender Online," Combine Resource Institution, March 2025, <https://www.combine.or.id/2025/03/08/hari-perempuan-internasional-2025-menyuarakan-kerentanan-dan-kekerasan-berbasis-gender-online/>.

² Juan Augusto Tatimu, "Analisis Yuridis Undang-Undang Tindak Pidana Kekerasan Seksual Berbasis Gender," *Lex Administratum* 12, no. 3 (2024): 1–12, <https://ejournal.unsrat.ac.id/v3/index.php/administratum/article/view/55676>.

fundamentally divergent legislative intents and distinct protected legal interests (*Rechtsgut*), none of which fully encapsulate the unique anatomy of sextortion. The forced application of these fragmented laws inevitably generates profound legal uncertainty, inconsistent judicial reasoning, and, distressingly, the secondary victimization of women who are frequently criminalized under draconian pornography statutes for merely being the subject of the extorted intimate material.

A critical examination of the current *state of the art* reveals that existing legal scholarship remains deeply polarized and fundamentally inadequate in addressing the hybridity of sextortion. Over the past five years, academic discourse in reputable journals has largely coalesced into two distinct camps. The first camp predominantly analyzes sextortion through a rigid cybercrime lens, emphasizing the illicit transmission of electronic data and treating the sexual nature of the content as merely incidental.^{3,4,5} Conversely, the second camp frames the issue exclusively within the paradigm of traditional sexual violence, focusing heavily on the absence of victim consent while underestimating the sophisticated digital extortion mechanisms utilized by organized perpetrators.^{6,7} By critically juxtaposing these dominant perspectives, this article argues that both approaches suffer from a significant theoretical blind spot. They fail to recognize that the distinct criminal liability of sextortion lies precisely in the symbiotic execution of its *actus reus* (the weaponization of digital content) and its *mens rea* (the specific intent to extort via sexual shaming). Thus, relying on prior studies exposes a persistent gap in the literature: the absence of a unified doctrinal framework capable of bridging cyber-extortion and gender-based sexual violence without diluting the gravity of either component.

³ Roberta Liggett O'Malley and Karen M. Holt, "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime," *Journal of Interpersonal Violence* 37, no. 1–2 (January 9, 2022): 258–83, <https://doi.org/10.1177/0886260520909186>.

⁴ Fikri Chandra Permana, "Pertanggungjawaban Pidana Pelaku 'Sektorsi' Dalam Kekerasan Berbasis Gender Online (KBGO)," *Jurist-Diction* 5, no. 3 (May 30, 2022): 883–98, <https://doi.org/10.20473/jd.v5i3.35776>.

⁵ Jordy Herry Christian, "Sektorsi: Kekerasan Berbasis Gender Online Dalam Paradigma Hukum Indonesia," *Binamulia Hukum* 9, no. 1 (April 4, 2023): 83–92, <https://doi.org/10.37893/jbh.v9i1.364>.

⁶ Aqila Shafiq Aryaputri and Handar Subhandi Bakhtiar, "Women as Victims of Online Gender-Based Violence in a Victimology Perspective," *PALAR: Pakuan Law Review* 12, no. 2 (May 2026): 177–96, <https://palar-fhukum.unpak.ac.id/index.php/palar/article/view/95>.

⁷ Sherly Nur Hidayah and Fariz Farrih Izadi, "Perlindungan Hukum Korban Kejahatan Pemerasan Seksual (Sextortion) Di Media Sosial Ditinjau Dari UU No. 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," *Bandung Conference Series: Law Studies* 5, no. 1 (January 23, 2025): 263–70, <https://doi.org/10.29313/bcsls.v5i1.16012>.

To bridge this pronounced theoretical and regulatory gap, it is imperative to move beyond the mechanical application of existing positive law and develop a nuanced criminal liability framework predicated on perpetrator-victim typologies. This article introduces an original conceptual framework constructed upon the synthesis of three fundamental legal pillars: (1) the theory of criminal responsibility, emphasizing the gradualization of culpability and the nuanced establishment of *mens rea* in digital environments; (2) victimological theory, specifically focusing on the asymmetry of harm and the distinct power dynamics inherent in gender-based coercion; and (3) the theory of responsive and adaptive regulation, which advocates for the cohesive restructuring of legal instruments to combat technology-facilitated crimes.⁸ Crucially, this research utilizes a purely normative and conceptual approach; it fundamentally rejects the necessity of statistical data or quantitative metrics to validate its claims, relying instead on rigorous doctrinal analysis, statutory interpretation, and the critical evaluation of legal principles to dismantle the existing regulatory ambiguities. By applying this qualitative legal analytical blade, the framework systematically addresses varying sextortion typologies—ranging from financially motivated schemes to relational coercion—and examines the diverse characteristics of perpetrators, thereby offering a highly adaptable methodology for evaluating criminal liability in complex cybercrimes.

Consequently, this article firmly posits the thesis that the eradication of sextortion and the substantive protection of female victims cannot be achieved through the fragmented enforcement of existing statutes; it strictly necessitates the immediate legislative formulation of a *sui generis* sextortion offense rooted in a gender-responsive paradigm. Throughout this manuscript, the central argument maintained is that treating sextortion as a mere subset of either general extortion or conventional pornography fundamentally mischaracterizes the offense and obstructs substantive justice. Ultimately, by elevating this national legal conundrum to the global discourse, this article provides critical theoretical and prescriptive insights. It not only proposes a definitive re-conceptualization of criminal liability for digital sexual extortion but also offers a comprehensive legislative blueprint that can serve as a global lesson learned for other jurisdictions struggling to harmonize their penal codes with the realities of modern online gender-based violence.

⁸ Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: Oxford University, 1992), Page, 100. <https://doi.org/10.1093/oso/9780195070705.001.0001>.

2. Research Questions

Despite the escalating incidence of online gender-based sextortion targeting women, the Indonesian criminal justice system suffers from a critical regulatory vacuum, resulting in a fragmented statutory framework and pervasive inconsistencies in law enforcement. This systemic deficiency raises fundamental jurisprudential issues concerning the doctrinal construction of criminal liability and the substantive adequacy of existing penal instruments in addressing sextortion as a distinct and highly complex manifestation of online gender-based violence (OGBV). To rigorously direct the analytical trajectory of the subsequent discussion, this study addresses the following primary legal research questions:

- a. How should the doctrinal framework of criminal liability for perpetrators of online gender-based sextortion be systematically constructed under Indonesian criminal law to resolve the prevailing regulatory fragmentation?
- b. To what extent does the integration of a gender-responsive paradigm within the current penal framework guarantee substantive justice and provide adequate legal protection for female victims against the asymmetric harm inherent in sextortion?

3. Research Methodology

This study employed a purely doctrinal legal research design to investigate the regulatory vacuum surrounding online gender-based sextortion within the Indonesian criminal justice system.⁹ The selection of this methodology was specifically justified to deconstruct the existing legal norms and conceptual frameworks, intentionally ensuring that the evaluation was firmly grounded in normative analysis without the utilization of statistical data or quantitative metrics. The investigation utilized a statutory approach and a conceptual approach. The statutory approach was operationalized to critically dissect the coherence, hierarchical consistency, and practical applicability of the current positive law in addressing the weaponization of intimate digital data. Simultaneously, the conceptual approach was systematically applied to construct a novel theoretical understanding of criminal liability, drawing from legal doctrines that address the hybrid nature of cyber-extortion, thereby bridging the gap where explicit statutory definitions were absent.

⁹ Sanne Taekema and Wibren van der Burg, "Methods of Doctrinal Research," in *Contextualising Legal Research* (Edward Elgar Publishing, 2024), 44–78, <https://doi.org/10.4337/9781035307395.00010>.

The core analytical corpus circumvented conventional generic classifications and directly interrogated the specific operative statutory instruments constituting the Indonesian penal framework. The primary regulatory texts meticulously analyzed included the Indonesian Criminal Code (KUHP), specifically scrutinizing Articles 368 and 369 governing traditional extortion and threats. Additionally, the study evaluated Law Number 1 of 2024 on Electronic Information and Transactions (ITE Law), focusing precisely on Article 27 paragraph (1) and Article 27B, alongside Law Number 44 of 2008 on Pornography (Article 4 paragraph (1) and Article 29), and Law Number 12 of 2022 on Sexual Violence Crimes (TPKS Law), particularly Article 4 paragraph (1) letter i and Article 14.

To ensure strict methodological rigor, transparency, and replicability, the collection of legal documents and scholarly literature was executed through targeted searches across reputable global academic databases, including HeinOnline, LexisNexis, and Scopus, as well as the official Indonesian government legal repository (JDIH). The search strategy incorporated precise Boolean operators and specific legal keywords, such as "sextortion," "online gender-based violence," "cyber-extortion," and "criminal liability." Strict inclusion and exclusion criteria were established to filter the gathered literature. The inclusion criteria mandated that all supporting legal literature—comprising peer-reviewed journal articles and authoritative legal treatises—must have been published within the preceding five years (2021–2026) to guarantee the contemporaneity and relevance of the academic discourse. Furthermore, to maintain the integrity of the doctrinal focus, any empirical studies heavily reliant on statistical field data were systematically excluded from the analysis.

Upon the systematic retrieval of the legal materials, the data were subjected to rigorous qualitative legal content analysis and deductive syllogism, moving entirely beyond mere descriptive summarization. The analytical blade operated primarily through a systematic interpretation of the statutory provisions, which involved critically juxtaposing the fragmented articles across the KUHP, ITE Law, Pornography Law, and TPKS Law to expose inherent normative contradictions and critical enforcement gaps. Furthermore, a teleological interpretation was rigorously applied to assess whether the original legislative intent behind these discrete statutes sufficiently accommodated the pressing necessity to protect female victims from the asymmetric harm of modern digital sextortion. Through this highly structured analytical procedure, the study successfully

generated valid, legally sound, and prescriptive conclusions regarding the urgent necessity of formulating a specific sextortion offense.

B. DISCUSSION

1. Qualification of Sextortion as a Complex Hybrid Crime within the Indonesian Criminal Justice System

The jurisprudential qualification of sextortion fundamentally challenges the conventional dichotomy within the Indonesian penal framework, which rigidly separates crimes against property from crimes against sexual decency. Rather than treating this phenomenon merely as a technological iteration of traditional extortion, a rigorous doctrinal evaluation reveals that sextortion must be classified as a complex, *sui generis* hybrid crime. The fundamental legal issue arises because the existing positive law structurally fails to accommodate offenses that simultaneously weaponize sexual exploitation and digital coercion to extract economic or relational advantages. Engaging in the current academic discourse, this analysis strongly refutes the dominant conservative legal scholarship—which frequently reduces sextortion to a mere violation of electronic transmission under the ITE Law—by arguing that such a reductionist perspective obfuscates the profound asymmetry of power and the specific gendered harm inflicted upon the victim. As Diba and Agustanti suggest, protecting victims requires transcending conventional extortion paradigms; however, this article extends their premise by asserting that legal protection can only be achieved if the justice system dogmatically recognizes the unique hybridization of technology and sexual violence inherent in the offense.¹⁰

To systematically deconstruct the criminal liability of the perpetrator, the operationalization of *actus reus* (the guilty act) and *mens rea* (the guilty mind) must be analyzed through the sequential anatomy of the crime, which encompasses grooming, deception, threat, and extortion. Unlike spontaneous conventional crimes, the *mens rea* in sextortion manifests as a continuous, premeditated acceleration of malicious intent. During the initial grooming and deception (catfishing) phases, the perpetrator orchestrates a sophisticated psychological manipulation to bypass the victim's digital boundaries, establishing the foundational *actus reus* of exploiting false trust. When the

¹⁰ Farah Diba and Rosalia Dika Agustanti, "Upaya Perlindungan Hukum Terhadap Korban Sekstorsi," *Jurnal Kertha Semaya* 13, no. 5 (2025): 910–25, https://repository.upnvj.ac.id/39362/1/2110611267_ArtikelKI.pdf.

perpetrator transitions to the threat and extortion phases, the intimate content is no longer merely private data; it is legally transformed into an instrument of psychological coercion. Permana correctly identifies these stages as central to online gender-based violence; nevertheless, this analysis sharpens that observation by emphasizing that the digital architecture allows the perpetrator to inflict infinite, permanent harm, thereby escalating the *actus reus* far beyond the temporal boundaries of traditional, offline extortion.¹¹

Furthermore, evaluating this crime exclusively through orthodox penal doctrines is grossly inadequate without deploying the analytical blade of legal feminism. When operationalized, feminist legal theory exposes that sextortion is not an isolated interpersonal conflict, but rather a digital manifestation of structural gender domination. The perpetrators deliberately weaponize existing patriarchal architectures and societal stigmas surrounding female sexuality to ensure the efficacy of their coercion. Consequently, the female victim is trapped in a paralyzing asymmetry of power; the threat of public exposure inflicts a disproportionate social devastation that forces compliance. By integrating this feminist perspective, it becomes evident that the current Indonesian legal framework—which often penalizes the victim under the Pornography Law for the existence of the explicit material—commits profound substantive injustice. The law effectively becomes an accomplice to the perpetrator by reinforcing the very gender injustice and social stigma the perpetrator exploits.

Ultimately, elevating this domestic regulatory vacuum to the global human rights discourse demonstrates that Indonesia's struggle with sextortion serves as a critical global lesson learned. The inability of a national legal system to protect its citizens from digital sexual extortion constitutes a direct violation of universal legal principles, specifically the right to privacy, bodily autonomy, and the right to be free from degrading treatment, as enshrined in the International Covenant on Civil and Political Rights (ICCPR) and the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). Therefore, this analysis concludes that mitigating sextortion requires a radical paradigm shift in criminal law. Jurisdictions globally, including Indonesia, must abandon fragmented regulatory approaches and enact a specific, gender-responsive penal provision that explicitly addresses the continuous, technology-facilitated weaponization

¹¹ Permana, "Pertanggungjawaban Pidana Pelaku 'Seksorsi' Dalam Kekerasan Berbasis Gender Online (KBGO)."

of human intimacy.

2. The Doctrinal Suitability and Comparative Efficacy of Criminal Law Regulations in Addressing Sextortion

The primary jurisprudential issue (*Issue*) currently paralyzing the Indonesian criminal justice system is the profound doctrinal mismatch between the hybrid characteristics of sextortion and the fragmented nature of existing positive law. Under the theoretical framework of adaptive regulation, legal instruments must evolve cohesively to anticipate and neutralize technological mutations of crime. However, the Indonesian regulatory approach remains severely anachronistic, mechanically forcing a complex digital gender-based offense into disparate, conventional statutory silos. A rigorous doctrinal evaluation (*Rule*) of the prevailing legal instruments—namely the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and the Sexual Violence Crimes Law (TPKS Law)—reveals critical normative gaps that systemic enforcement currently fails to bridge.

Applying a critical analytical lens (*Application*), the forced operationalization of the KUHP (specifically Articles 368 on extortion and 369 on threats) is fundamentally flawed because these provisions are inherently anchored in property-centric doctrines. They strictly require the element of material deprivation and are jurisprudentially incapable of recognizing the intangible, yet devastating, weaponization of digital intimacy. Furthermore, the application of the ITE Law (Article 27 paragraph 1 and Article 27B) exposes a dangerous ideological bias. The ITE Law operates predominantly on the legal interest (*Rechtsgut*) of preserving public morality (*kesusilaan*), rather than safeguarding individual bodily autonomy. By operationalizing victimological theory, it becomes starkly evident that this morality-centric approach frequently backfires, triggering severe secondary victimization. Law enforcement frequently misinterprets the victim's coerced digital footprint as a violation of public decency, thereby threatening the victim with criminalization.¹² While the TPKS Law (Articles 4 and 14) introduces progressive, gender-responsive terminology for electronic-based sexual violence, it doctrinally bifurcates the sexual element from the targeted economic or relational extortion element.¹³ In this context, this analysis confirms the observations of Christian (2023), who identifies this

¹² "Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, LNRI Tahun 2024 Nomor 1" (2024).

¹³ JDIH BPK, "Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," 2022.

regulatory fragmentation; however, this article critically extends his thesis by arguing that mere harmonized interpretation by judges is grossly insufficient. Without a fundamental statutory reform that amalgamates these elements into a single offense, the principle of *lex certa* (legal certainty) remains violated.¹⁴

To elevate this domestic regulatory vacuum into a global discourse, a comparative qualitative analysis of international jurisdictions is imperative. As delineated in Table 1, global responses to sextortion currently bifurcate into three dominant regulatory paradigms: the multi-offense model, the integrated sexual offenses model, and the specialized cybercrime model.

Table 1. Comparison of International Regulations on Sextortion

Country	Specific Sextortion Offence	Main Legal Instruments	Regulatory Approach	Maximum Penalty
Indonesia	No specific offence; regulation remains fragmented across several criminal provisions	Indonesian Criminal Code Articles 368–369; Electronic Information and Transactions Law Articles 27 and 27B; Sexual Violence Crimes Law Articles 4 and 14	Multi-offence approach, covering extortion, threats, and sexual exploitation	12 years imprisonment and/or a fine of IDR 100 million
Australia	No specific sextortion offence, but revenge porn is specifically regulated	<i>Crimes Act</i> ; revenge porn provisions; <i>Telecommunications Act</i> ; cyberstalking provisions	Multi-offence approach, covering blackmail, revenge porn, and cyberstalking	Up to 5 years imprisonment per offence
United States	No specific sextortion offence, but enforcement is among the strongest globally	18 U.S.C. § 875 on extortion; communications legislation; federal child exploitation laws	Multi-offence approach; the Department of Justice actively prosecutes numerous cases	Extortion: up to 20 years imprisonment
Canada	In the process of specific legislation in 2025	<i>Criminal Code</i> Section 346 on extortion; Section 162.1 on intimate images; child protection provisions	Multi-offence approach; strengthening laws on online sextortion	Extortion: life imprisonment; distribution of intimate images: 5 years imprisonment
England and Wales	No specific sextortion offence, but blackmail is specifically regulated	<i>Theft Act 1968</i> Section 21 on blackmail; <i>Sexual Offences Act 2003</i> ; <i>Online Safety Act 2023</i>	Multi-offence approach, covering blackmail and gender-based harassment	Blackmail: up to 14 years imprisonment

¹⁴ Jordy Herry Christian, “Sekstorsi: Kekerasan Berbasis Gender Online Dalam Paradigma Hukum Indonesia.”

Kenya	In the process of regulation through a proposed amendment to the <i>Sexual Offences Act</i>	<i>Sexual Offences Act</i> through proposed amendment; <i>Computer Misuse and Cybercrimes Act</i>	Legal reform toward a gender-based specific offence	Not yet determined; still under consultation
Norway	No specific sextortion offence, but enforcement exists	<i>Sexual Offences Act</i> ; <i>General Criminal Code</i> on extortion and sexual harassment	Multi-offence approach, focusing on sexual violence involving power imbalance	Example from a 2019 case: 5 years imprisonment for sexual abuse
India	In the process of specific legislation in several states	<i>Indian Penal Code</i> ; <i>Information Technology Act</i> ; state-level cyber laws	Varies across states; legal reform is ongoing	Varies and has not been nationally standardized

Source: Processed from a comparative analysis of international criminal law regulations.

Through the lens of adaptive regulation theory, Indonesia's reliance on the multi-offense approach—mirroring Australia and the UK—exacerbates legal uncertainty due to the absence of specific blackmail or specialized revenge pornography statutes that those Commonwealth nations possess. Conversely, analyzing the specialized legislative trajectories observed in the United States and Canada (slated for 2025) offers a superior doctrinal blueprint. Refuting the premise that broad, existing cyber laws are adequate, this comparative analysis demonstrates that specialized frameworks directly recognizing the intersection of gender-based coercion and digital extortion yield significantly higher enforcement coherence. This aligns with Root's (2023) assertion regarding the global urgency for explicit legal protections; however, applying this to the Indonesian context reveals that importing foreign statutes must be coupled with structural dismantling of the domestic morality-based paradigms.¹⁵

The severe practical consequences of this doctrinal inadequacy are empirically reflected in global law enforcement practices, as detailed in Table 2.

¹⁵ Rebecca Root, "Pressure Builds Worldwide for Legal Protection Against Sextortion," International Bar Association, 2023, <https://www.ibanet.org/Human-rights-news-Feb-Mar-2024>.

Table 2. International Practices in Law Enforcement Regarding Sextortion

Country	Reporting Level	Main Law Enforcement Practices	Main Challenges	Prosecution Success Rate
Indonesia	Very low; approximately 17% of victims report cases	Prosecution relies on multiple legal provisions; enforcement remains case-based, including decisions from the Pasir Pangaraian District Court and Bandung District Court	Fragmented regulation; limited digital forensic capacity; potential criminalization of victims under pornography laws	Low; cases remain sporadic and inconsistent
Australia	Increasing; around 80% of reports in several states	Multi-offence prosecution; active role of the eSafety Commissioner; specific regulation on revenge porn	Inter-jurisdictional coordination; complex digital forensics; psychological barriers faced by victims	Moderate and increasing; average penalties range from 2 to 5 years imprisonment
Canada	Increasing, especially in cases involving children	Active prosecution; 2025 amendments addressing online sextortion; multi-offence approach	Cross-border jurisdiction; high evidentiary standards; availability and reliability of digital evidence	High for extortion cases, estimated at above 80%; expected to improve further after the 2025 legislative reforms
England and Wales	Moderate, approximately 40–60%	Blackmail prosecution; sentencing guidelines issued in April 2025 for blackmail, kidnapping, and false imprisonment	Social stigma faced by victims; complex electronic evidence; cross-border jurisdiction under data protection rules	Moderate; conviction rate for blackmail cases is above 60%
Kenya	Very low; estimated at 10–15% reporting rate	INTERPOL Operation Contender 3.0 in 2025; 260 arrests and more than 1,400 victims identified; focus on advocacy-driven cases ¹⁶	Undefined specific offence; lack of digital infrastructure; gender-based stigma; corruption in law enforcement	Very low; INTERPOL operations require external support
Uganda	Very low	INTERPOL Operation Contender 3.0; limited standalone prosecution capacity	Absence of a specific legal framework; limited technical capacity; lack of specialized units	Very low without international support
United States	Increasing, supported by active Department of Justice awareness campaigns	Department of Justice prosecutes dozens of cases annually; integrated federal approach; strong cybercrime unit capacity	Cross-border jurisdiction; federal–state coordination; victim-related barriers	Highest globally, with conviction rates estimated above 85%

¹⁶ INTERPOL, “260 Suspected Scammers Arrested in Pan-African Cybercrime Operation,” INTERPOL, 2025, <https://www.interpol.int/News-and-Events/News/2025/260-suspected-scammers-arrested-in-pan-african-cybercrime-operation>.

Norway	Moderate; the 2019 case received international media attention	Prosecution based on the sexual offences framework; offender-centric approach focusing on corruption and abuse of power	Psychological barriers faced by victims; complexity of proving power imbalance; international dimension	Moderate; for example, a 2019 sexual abuse case resulted in 5 years imprisonment
--------	--	---	---	--

Source: Processed from comparative international law enforcement practices on sextortion.

While this study strictly utilizes a normative legal methodology and does not rely on statistical inferences to establish its primary claims, the data presented in Table 2 serves as crucial empirical context illustrating a profound normative failure. The dismal 17% reporting rate in Indonesia, juxtaposed with the international findings from INTERPOL’s Operation Contender 3.0 (which identified expansive cyber-scam networks across Africa in 2025), highlights a systemic collapse in victim protection. Viewed through a victimological lens, the lack of a unified legal reference point creates an insurmountable psychological barrier to justice. When law enforcement officers are forced to arbitrarily select prosecutorial articles based on subjective assessments of fragmented laws, the legal system institutionalizes unpredictability.¹⁷

Consequently (*Conclusion*), the substantive integration of adaptive regulation and victim protection demands the immediate abandonment of Indonesia’s fragmented multi-offense model. The persistent reliance on conventional penal instruments fundamentally fails to capture the asymmetric harm of sextortion, necessitating targeted, gender-responsive legislative intervention to restore both legal certainty and substantive justice.

3. The Jurisprudential Disparity and Practical Failure of Law Enforcement Against Sextortion in Indonesia

The theoretical fragmentation of Indonesia’s regulatory framework inevitably precipitates a profound systemic failure in judicial practice. In the absence of a *sui generis* statute specifically criminalizing sextortion, the principle of *lex certa* (legal certainty) is severely compromised. Law enforcement agencies and the judiciary are compelled to arbitrarily select prosecutorial instruments, resulting in wildly divergent adjudications for fundamentally identical crimes. This doctrinal crisis is explicitly illustrated by juxtaposing two distinct court rulings that handled cyber-extortion involving intimate digital material. By critically analyzing the *ratio decidendi* (the rationale for the decision)

¹⁷ Bruhan Makong, “260 Suspected Cyber Scammers in 14 African Countries Including Kenya Arrested Over Sextortion,” Capital Group Limited, September 2025, <https://capitalfm.africa/260-suspected-cyber-scammers-in-14-african-countries-including-kenya-arrested-over-sexortion/>.

in these cases, it becomes evident that the current legal apparatus is structurally incapable of delivering substantive justice for victims of online gender-based violence.

The first jurisprudential anomaly is observed in the Pasir Pangaraian District Court Decision Number 229/Pid.Sus/2021/PN Prp. In this case, the perpetrators systematically trapped the victim via an explicit video call, covertly recorded the interaction, and subsequently weaponized the digital footage to extort financial assets.¹⁸ The adjudicating panel exclusively applied the ITE Law, framing the offense primarily as an illicit transmission of electronic data. While the judges correctly identified the *mens rea* (the malicious intent to extort) and the *actus reus* (the digital transmission of threats), the imposed sentence of merely one year and three months imprisonment constitutes a gross violation of penal proportionality. By evaluating this ruling through the lens of victimological theory, the court fundamentally failed to recognize the permanent, asymmetric harm inflicted upon the victim. A nominal prison sentence is drastically disproportionate to the irreversible psychological devastation and permanent "social death" caused by the perpetual risk of the digital footprint being disseminated across cyberspace.

Conversely, the Bandung District Court Decision Number 856/Pid.B/2019/PN.Bdg exposes a contradictory judicial approach. Confronted with an identical *modus operandi*—extortion facilitated by the threat of distributing a recorded sexual video call—the prosecution and the judiciary bypassed the ITE Law entirely, opting instead to charge the defendant under the conventional extortion provisions of the Indonesian Criminal Code (KUHP).¹⁹ This application demonstrates a dangerous reductionist paradigm. By prosecuting the act solely as a conventional property crime, the court effectively erased the gender-based sexual violence dimension from the legal narrative. The fundamental legal error in this approach is the failure to acknowledge that the intimate content was not merely a passive object used for leverage; rather, the unauthorized recording and threatened exposure constituted an active, continuous violation of the victim's bodily autonomy and sexual integrity.

When these two rulings are critically dialogued, they demonstrate a pervasive jurisprudential paralysis. The judiciary is currently forced to amputate the crime to fit

¹⁸ "Putusan Pengadilan Negeri Pasir Pangaraian Nomor 229/Pid.Sus/2021/PN Prp" (2021).

¹⁹ Aliea Aqshalina Apriliyani, *Analisis Putusan Pengadilan Negeri Bandung Nomor 856/Pid.B/2019/PN.Bdg Tentang Pelaku Pemerasan Dan Pengancaman Video Call Sex Dalam Aplikasi WhatsApp Perspektif Hukum Pidana Islam* (Tesis: UIN Sunan Gunung Djati Bandung, 2023). Page, 123.

inadequate statutes: the ITE Law captures the digital medium but minimizes the extortionate coercion, whereas the KUHP captures the financial extortion but entirely dismisses the digital sexual exploitation. This domestic judicial inconsistency serves as a critical global lesson learned regarding the dangers of legislative stagnation. International legal standards, including the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), mandate state actors to comprehensively protect women from all manifestations of gender-based violence, encompassing its digital iterations. When a national jurisdiction systematically renders the sexual dimension of a cybercrime invisible, or treats the permanent digital subjugation of a woman as a minor misdemeanor, the state inherently fails its international human rights obligations.

Ultimately, the empirical reality of law enforcement in Indonesia incontrovertibly proves that mere judicial interpretation is insufficient to bridge the regulatory vacuum. To eradicate this dangerous disparity and guarantee proportional justice, the legislature must urgently enact a specialized, integrated sextortion provision. This statute must concurrently recognize the financial coercion, the weaponization of digital technology, and the severe asymmetry of gender-based harm, thereby ensuring that perpetrators face criminal liability commensurate with the multidimensional devastation they inflict.

4. Multidimensional Impediments to Law Enforcement and the Structural Phenomenon of Secondary Victimization

The prosecution of online gender-based sextortion in Indonesia is currently paralyzed by a confluence of normative, practical, and structural impediments. From a normative legal perspective, the prevailing legislative vacuum engenders profound institutional paralysis. Rather than merely possessing an abundance of overlapping statutes, law enforcement agencies are fundamentally deprived of a unified prosecutorial blueprint. Consequently, investigators are forced into a precarious exercise of legal maneuvering, attempting to mold a complex, hybrid cyber-extortion offense to fit the rigid evidentiary thresholds of either conventional property crimes or generic morality offenses. As Hidayah and Izadi conceptualize, this fractured legal foundation prevents the formulation of standardized investigative protocols, severely compromising the drafting of precise indictments and routinely resulting in the dismissal of charges due to obscure legal reasoning.²⁰ This systemic ambiguity directly contravenes the principle of *lex certa*,

²⁰ Hidayah and Izadi, "Perlindungan Hukum Korban Kejahatan Pemerasan Seksual (Sextortion) Di Media Sosial Ditinjau Dari UU No. 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual."

effectively transforming the judicial process into an unpredictable lottery for the victims.

Transitioning to the practical domain, the efficacy of law enforcement is profoundly undermined by formidable sociological and technological barriers. Without relying on quantitative metrics, a conceptual victimological analysis reveals that sextortion generates a massive "dark figure of crime." The vast majority of incidents remain unreported not due to statistical anomalies, but because of a paralyzing chilling effect induced by intense societal stigma and the asymmetrical power dynamics inherent in gender-based violence.²¹ Victims are acutely aware that the digital architecture allows perpetrators to execute their threats instantaneously and permanently. Furthermore, this domestic reluctance is exacerbated by significant transnational technological hurdles. Sextortion networks frequently exploit extraterritorial jurisdictions, advanced encryption, and decentralized digital anonymity. When these globalized cyber-tactics confront domestic law enforcement agencies—which often suffer from a severe deficit in sophisticated digital forensic capabilities—the resulting evidentiary chain of custody is frequently compromised, rendering the prosecution incapable of proving the *actus reus* beyond a reasonable doubt in a court of law.

Most alarmingly, the existing legal architecture harbors a severe structural impediment that institutionalizes secondary victimization. Evaluated through the analytical blade of legal feminism, certain conservative legal instruments—most notably the Pornography Law—operate as patriarchal architectures that actively endanger the victim. Because these morality-based statutes inherently criminalize the mere production or possession of sexually explicit material without rigorously interrogating the coercive context of its creation, female victims face the imminent peril of being prosecuted as co-conspirators or perpetrators of obscenity. In this grotesque distortion of justice, the law fundamentally mischaracterizes the coerced digital footprint as a consensual moral violation.

Consequently, the state inadvertently assumes the role of an accomplice to the extortionist. The very legal apparatus designated to protect the victim becomes the ultimate instrument of the perpetrator's threat, ensuring the victim's silence through the looming terror of state-sanctioned criminalization. To dismantle these multidimensional obstacles and align with universal human rights standards, it is an absolute necessity to

²¹ Hidayah and Izadi.

reform the domestic legal framework. The legislature must decisively enact a specialized penal provision that explicitly immunizes coerced victims from prosecution and equips law enforcement with the precise doctrinal tools required to combat the transnational, gendered complexities of digital extortion.

C. CONCLUSION

The doctrinal construction of criminal liability for online gender-based sextortion in Indonesia is currently paralyzed by a fragmented statutory framework, as reliance on disparate conventional property and cyber laws fundamentally fails to capture the hybrid nature of digital sexual extortion. Consequently, the existing penal apparatus is substantively inadequate, failing to provide legal certainty while inadvertently exposing female victims to the severe risk of secondary victimization under morality-centric statutes. To resolve this jurisprudential crisis and eradicate the systemic disparity in law enforcement, the Indonesian legislature must urgently abandon the current multi-offense paradigm. Enacting a *sui generis*, gender-responsive penal provision is absolutely imperative to accurately criminalize the specific asymmetric harm of technology-facilitated coercion and guarantee comprehensive substantive justice for victims.

REFERENCES

- Apriliani, Aliea Aqshalina. *Analisis Putusan Pengadilan Negeri Bandung Nomor 856/Pid.B/2019/PN.Bdg Tentang Pelaku Pemerasan Dan Pengancaman Video Call Sex Dalam Aplikasi WhatsApp Perspektif Hukum Pidana Islam*. Tesis: UIN Sunan Gunung Djati Bandung, 2023.
- Aryaputri, Aqila Shafiq, and Handar Subhandi Bakhtiar. "Women as Victims of Online Gender-Based Violence in a Victimology Perspective." *PALAR: Pakuan Law Review* 12, no. 2 (May 2026): 177-96. <https://palar-fhukum.unpak.ac.id/index.php/palar/article/view/95>.
- Ayres, Ian, and John Braithwaite. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University, 1992. <https://doi.org/10.1093/oso/9780195070705.001.0001>.
- Combine Resource Institution. "Hari Perempuan Internasional 2025: Menyuarakan Kerentanan Dan Kekerasan Berbasis Gender Online." Combine Resource Institution, March 2025. <https://www.combine.or.id/2025/03/08/hari-perempuan-internasional-2025-menyuarakan-kerentanan-dan-kekerasan-berbasis-gender-online/>.
- Diba, Farah, and Rosalia Dika Agustanti. "Upaya Perlindungan Hukum Terhadap Korban Seksorsi." *Jurnal Kertha Semaya* 13, no. 5 (2025): 910-25. https://repository.upnvj.ac.id/39362/1/2110611267_ArtikelKI.pdf.
- Hidayah, Sherly Nur, and Fariz Farrih Izadi. "Perlindungan Hukum Korban Kejahatan

- Pemerasan Seksual (Sextortion) Di Media Sosial Ditinjau Dari UU No. 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual." *Bandung Conference Series: Law Studies* 5, no. 1 (January 23, 2025): 263–70. <https://doi.org/10.29313/bcsls.v5i1.16012>.
- INTERPOL. "260 Suspected Scammers Arrested in Pan-African Cybercrime Operation." INTERPOL, 2025. <https://www.interpol.int/News-and-Events/News/2025/260-suspected-scammers-arrested-in-pan-African-cybercrime-operation>.
- JDIH BPK. "Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual," 2022.
- Jordy Herry Christian. "Sekstorsi: Kekerasan Berbasis Gender Online Dalam Paradigma Hukum Indonesia." *Binamulia Hukum* 9, no. 1 (April 4, 2023): 83–92. <https://doi.org/10.37893/jbh.v9i1.364>.
- Makong, Bruhan. "260 Suspected Cyber Scammers in 14 African Countries Including Kenya Arrested Over Sextortion." Capital Group Limited, September 2025. <https://capitalfm.africa/260-suspected-cyber-scammers-in-14-african-countries-including-kenya-arrested-over-sex-tortion/>.
- O'Malley, Roberta Liggett, and Karen M. Holt. "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime." *Journal of Interpersonal Violence* 37, no. 1–2 (January 9, 2022): 258–83. <https://doi.org/10.1177/0886260520909186>.
- Permana, Fikri Chandra. "Pertanggungjawaban Pidana Pelaku 'Sekstorsi' Dalam Kekerasan Berbasis Gender Online (KBGO)." *Jurist-Diction* 5, no. 3 (May 30, 2022): 883–98. <https://doi.org/10.20473/jd.v5i3.35776>.
- Putusan Pengadilan Negeri Pasir Pangaraian Nomor 229/Pid.Sus/2021/PN Prp (2021).
- Root, Rebecca. "Pressure Builds Worldwide for Legal Protection Against Sextortion." International Bar Association, 2023. <https://www.ibanet.org/Human-rights-news-Feb-Mar-2024>.
- Taekema, Sanne, and Wibren van der Burg. "Methods of Doctrinal Research." In *Contextualising Legal Research*, 44–78. Edward Elgar Publishing, 2024. <https://doi.org/10.4337/9781035307395.00010>.
- Tatimu, Juan Augusto. "Analisis Yuridis Undang-Undang Tindak Pidana Kekerasan Seksual Berbasis Gender." *Lex Administratum* 12, no. 3 (2024): 1–12. <https://ejournal.unsrat.ac.id/v3/index.php/administratum/article/view/55676>.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, LNRI Tahun 2024 Nomor 1 (2024).