American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN : 2378-703X
Volume-10, Issue-01, pp-126-132
www.ajhssr.com
Research Paper Open Access

Legal Consequences for Perpetrators of Love Scamming

Anak Agung Sagung Laksmi Dewi[1], Anak Agung Ngurah Adhi Wibisana[2]
Faculty of Law, Universitas Warmadewa, Denpasar, Bali

ABSTRACT: Love scamming is a form of cybercrime classified as computer-related fraud and is carried out through the construction of fictitious digital personas, emotional approaches, and psychological manipulation to induce victims to transfer money or provide other benefits. In Indonesia, the trend of love scamming cases shows an increase, with financial losses reaching tens to hundreds of millions of rupiah, accompanied by psychological impacts such as trauma, shame, and loss of trust. However, to date, there is no specific regulation governing love scamming as a distinct criminal offense, so its handling relies on a combination of provisions in the Criminal Code (KUHP) and sectoral regulations. This study aims to analyze the legal regulation of love scamming within the Indonesian legal system and to identify the forms of criminal sanctions that may be imposed on perpetrators. The research method employs normative legal research with statutory, conceptual, and case approaches. Primary legal materials include the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), the Anti-Money Laundering Law (UU TPPU), as well as court decisions related to online fraud; secondary materials consist of literature and institutional reports; and tertiary materials serve as terminological reinforcement. The results show that the regulation of love scamming remains fragmentary, primarily relying on Article 378 of the Criminal Code and provisions of the Electronic Information and Transactions Law (Article 28 paragraph (1) and Article 35 in conjunction with Article 51), with the possible application of the Sexual Violence Crimes Law (UU TPKS), the Personal Data Protection Law, and the Anti-Money Laundering Law depending on the elements of the act. Normatively, criminal sanctions are available in a tiered manner, but their effectiveness is constrained by challenges in digital evidence, limited forensic capacity, and the absence of specific sentencing standards.

KEYWORDS: *Love Scamming, Romance Fraud, Cybercrime, Electronic Information And Transactions Law (UU ITE), Criminal Sanctions, Indonesia*

I. INTRODUCTION

Love scamming falls within the category of cybercrime classified as computer-related fraud. According to Brenner, cybercrime has specific characteristics such as anonymity, cross-border nature, and the use of technology to facilitate criminal acts (Brenner, S. 2010). In the context of love scamming, perpetrators typically construct fictitious digital personas and employ emotional approaches with the aim of deceiving victims gradually. This modus operandi makes love scamming more complex than conventional fraud. The phenomenon of love scamming in Indonesia shows an increasing trend each year. Reports from the Ministry of Communication and Informatics (Kominfo) as well as various empirical studies indicate that the financial losses suffered by victims can reach tens to hundreds of millions of rupiah (Kumalasari, N., & Wijaya,2024). Victims generally experience not only economic losses but also psychological impacts such as emotional trauma, shame, and a loss of trust in digital interactions (Whitty,2017).

Although love scamming has become one of the frequently occurring forms of digital crime, Indonesia has not yet enacted specific regulations that explicitly govern this offense. The Indonesian legal system currently addresses it through general provisions in the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). According to Sibarani, the absence of specific rules causes law enforcement officers to rely on interpretations of provisions on fraud, identity falsification, or the dissemination of electronic data to prosecute perpetrators (Sibarani, R.2020). In the Criminal Code, the article most frequently used to address love scamming is Article 378 concerning fraud. However, the elements contained in this article are often considered inadequate because they do not specifically regulate fraudulent activities conducted through electronic systems. This view is consistent with Marpaung's opinion, which emphasizes that the development of digital fraud modalities requires regulations that are more responsive and adaptive to technological advances (Marpaung,2018).

Meanwhile, the Electronic Information and Transactions Law provides a clearer legal basis through Article 28 paragraph (1) and Article 35 concerning data manipulation and electronic identity falsification.

According to Adi, both articles can be used to prosecute perpetrators of love scamming, but challenges remain in terms of evidence, particularly in tracing perpetrators who exploit virtual private networks (VPNs), anonymous accounts, and foreign-based devices (Adi, R., 2021). This indicates that law enforcement against love scamming requires a multidisciplinary approach and international coordination. From a criminological perspective, love scamming constitutes a crime that exploits victims' emotional vulnerabilities. Perpetrators typically target individuals who are lonely, emotionally vulnerable, or seeking romantic relationships (Whitty & Garry, 2015). Through psychological manipulation techniques such as emotional grooming, perpetrators gradually build trust before requesting money under various pretexts. Whitty's research shows that victims often fail to recognize signs of fraud due to strong emotional bonds (Whitty, M. T.,2018).

Another legal issue concerns the application of sanctions against perpetrators. In Indonesia, sanctions for love scamming perpetrators depend on the articles used as the legal basis in judicial proceedings. Perpetrators may be subject to imprisonment, fines, or both, yet consistency in law enforcement practice has not been achieved. According to Siregar, the lack of regulatory clarity and evidentiary procedures often results in perpetrators receiving lighter sentences than warranted by the harm suffered by victims (Siregar, 2022). In several countries, love scamming has been specifically regulated as a form of organized and cybercrime. For example, Cross's research shows that Australia applies a "fraud-specific framework" that emphasizes victim protection and loss recovery (Cross, 2019). This comparison indicates that Indonesia needs to strengthen its regulatory framework to provide more optimal legal protection.

The absence of specific regulations also affects victim recovery efforts. In many cases, victims encounter difficulties in obtaining compensation because funds have been transferred through international channels or laundered through intermediary accounts. Rahardjo's research shows that mechanisms for restitution and compensation for victims of cybercrime in Indonesia remain very limited, mainly due to the lack of legal instruments that specifically regulate the protection of digital crime victims (Cross, 2019).Based on these various issues, research on the legal consequences of love scamming, particularly concerning legal regulation and sanctions for perpetrators, is of significant importance. This research not only contributes to the development of cyber law and criminal law theory but also provides practical recommendations for policymakers and law enforcement authorities. Through comprehensive analysis, this study is expected to map existing legal gaps and offer directions for regulatory reform that are more responsive to the development of digital crime.

Based on the background discussed above, the research questions in this study are as follows:

1. How is the legal regulation of the crime of love scamming structured within the Indonesian legal system?
2. What forms of criminal sanctions can be imposed on perpetrators of love scamming based on the applicable legal provisions in Indonesia?.

II. METHODE

This study is a normative legal research focusing on the analysis of legal norms and provisions governing the crime of love scamming in Indonesia. The approaches employed include the statutory approach, the conceptual approach, and the case approach, aimed at examining the legal regulation of online relationship-based fraud, cybercrime, digital identity, and their legal implications in law enforcement practice (Christiani, T. A., 2015). The research data sources consist of primary, secondary, and tertiary legal materials collected through library research. Primary legal materials include the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), the Anti-Money Laundering Law (UU TPPU), as well as court decisions related to online fraud. Secondary legal materials comprise books, journal articles, and official reports from relevant institutions discussing cybercrime and romance fraud, while tertiary legal materials are used to strengthen terminological and conceptual understanding. All materials are analyzed qualitatively to produce a systematic and argumentative study.

III. RESULT AND DISCUSSION

3.1 Legal Regulation of the Crime of Love Scamming within the Indonesian Legal System

The phenomenon of love scamming, or romance-based fraud, constitutes a form of cybercrime that has shown a significant increase in Indonesia alongside the expanding penetration of digital technology, social media, and online dating applications (Putri & Saraswati2024). Love scamming relies on the manipulation of interpersonal relationships through the creation of fictitious romantic relationships to obtain economic or sexual benefits, by exploiting psychological vulnerabilities, loneliness, domestic problems, or unstable emotional conditions of victims (Niman & Rothhaar,2023). This crime is carried out through persuasive communication strategies that lead victims to perceive the relationship as a genuine and meaningful romantic bond worth maintaining (Whitty, 2018). The modus operandi employed by perpetrators is systematic in nature. Offenders use false identities, stolen photographs, attractive profiles, and fabricated humanitarian narratives, for example claiming to be foreign nationals with prestigious professions such as doctors, seafarers, or members of international military forces (Whitty & Buchanan, 2016). Perpetrators actively exploit social media and dating

applications to identify targets, infiltrate victims' personal lives, and deceive them through structured, persuasive, and emotionally charged communication patterns (Sultan, & Kursiswanti,2024). They construct false emotional relationships to manipulate victims into sending money under various fictitious pretexts, such as shipping costs, import taxes, or medical expenses. Romance scam perpetrators consistently build narratives of love, trust, and emotional dependence prior to engaging in financial exploitation (Sultan, & Kursiswanti,2024).

The stages of online romance fraud generally include the creation of fake profiles, the development of intensive relationships, grooming processes to establish emotional attachment, the fabrication of false crises, and subsequent requests for money or sexual exploitation (Kumalasari & Wijaya, 2024). Faber emphasizes that perpetrators employ repetitive persuasive scripts resembling covert commercial transactions, positioning victims as parties who "purchase" the relationship promised by the offender. Within this framework, love scamming is not merely financial fraud but also a form of well-planned psychological and economic manipulation (Faber,2024).The success of this modus operandi is strongly influenced by the characteristics of digital communication. Computer-mediated interaction creates hyperpersonal relationships that blur victims' vigilance, as interactions occur without physical contact and the perpetrator's self-presentation can be entirely fabricated (Faber,2024). Communication theory perspectives reinforce this understanding. Interpersonal Deception Theory explains how perpetrators control self-presentation, conceal intentions, and regulate information flow so that victims are unable to detect deception. Psychological findings indicate that individuals with high levels of trust, impulsivity, and strong needs for affection are more susceptible to manipulation through digital relationships (Niman & Rothhaar,2023). Love scamming also has dimensions of Online Gender-Based Violence (Kekerasan Berbasis Gender Online/KBGO). Many cases in Indonesia place women as the most vulnerable group to digital romance fraud, both economically and psychologically. Emotional manipulation is carried out gradually, beginning with the creation of an idealized identity and escalating to threats of disseminating intimate images (sextortion), resulting in significant psychological and material harm. The increase in KBGO cases related to digital romance fraud indicates that women frequently experience intimidation, threats, and extortion in online relationships (Kumalasari & Wijaya, 2024). Social constructions of femininity, stigma against unmarried women, and emotional stereotypes further exacerbate this vulnerability. In numerous cases, female victims suffer profound emotional distress due to betrayal of trust and moral stigma imposed by their social environment (Shaari, et.al, 2019).

From the perspective of positive law, there is no specific regulation governing love scamming within the Indonesian legal system. The classical Criminal Code (KUHP), through Article 378, does regulate fraud based on deceit, falsehoods, or false identities, but this provision does not fully capture the complexity of fraud conducted through digital relationships (Solihin, R., & Zuhri, A., 2024). The 2023 National Criminal Code likewise does not provide a specific category for fraud committed through emotional or online relationships, resulting in continued reliance by law enforcement on broad interpretations of general fraud and extortion provisions Sofiana, Purnomo, & Rosita, 2025). The Electronic Information and Transactions Law (UU ITE) is the legal instrument most frequently used to prosecute love scamming perpetrators, particularly through Article 28 paragraph (1) concerning the dissemination of false information and Article 35 in conjunction with Article 51 regulating digital identity manipulation. However, there is disharmony between the KUHP and the UU ITE in their application, leading to inconsistencies in judicial practice. The Sexual Violence Crimes Law (UU TPKS) may be applied when love scamming involves sextortion, yet this regulation has not explicitly categorized digital romance fraud as a form of technology-based sexual violence.Other legal instruments, such as the 2022 Personal Data Protection Law, provid e only an initial framework for data protection. Its implementation remains limited due to the absence of an independent supervisory authority and weak enforcement in cases of data misuse.This condition increases the risk of victims becoming targets of image-based sexual extortion (Duha,2024).

Law enforcement faces significant structural obstacles. Perpetrators are difficult to trace due to the use of false identities, anonymous accounts, VPNs, and overseas servers (Qoir & Ichsan, 2025). Digital evidence is volatile, easily lost, and often located on global platforms beyond Indonesian jurisdiction. In addition, many victims are reluctant to report incidents due to shame, trauma, limited digital literacy, and lack of knowledge regarding reporting mechanisms. Law enforcement officers also frequently lack technical capacity in digital forensics, resulting in many cases being handled suboptimally. In terms of victim protection, the UU ITE does not comprehensively regulate the rights of love scamming victims. Protection largely depends on Law No. 31 of 2014 on Witness and Victim Protection, which provides rights to confidentiality of identity, psychological support, and security guarantees (Bimantari, et al, 2025). However, practice shows that psychosocial recovery services, compensation, and personal data protection are not consistently provided. Many victims experience revictimization due to data leaks, dissemination of private images, or intimidation by perpetrators.

The economic dimension of love scamming is clearly reflected in reports from the Financial Transaction Reports and Analysis Center (PPATK). The January 2025 report recorded 8,146 analyses of suspicious financial transactions related to digital relationship-based fraud. These figures continued to rise in February (9,705), March (11,647), April (8,707), May (9,794), and June 2025 (8,821). Reports from August and

September 2025 even revealed patterns of transaction layering and the use of mule accounts, indicating the involvement of transnational organized crime networks (13,044 and 10,673 analyses) (PPATK,2025). These data demonstrate that love scamming is not merely interpersonal fraud but is closely linked to money laundering offenses requiring cross-jurisdictional cooperation. Based on these findings, multi-level prevention and enforcement strategies are required. Non-penal approaches include enhancing digital literacy, educating the public about romance fraud schemes, restricting anonymous accounts through digital identity verification, and improving law enforcement capacity in understanding modern manipulation techniques (Temcharoenkit & Rani, 2025). Penal approaches require the establishment of specific regulations on love scamming to harmonize the KUHP and UU ITE, clarify offense elements, regulate digital jurisdiction, and provide evidentiary standards suited to the nature of cybercrime. Furthermore, international cooperation must be strengthened, as many perpetrators originate from foreign syndicates beyond the reach of Indonesian authorities.

Overall, the Indonesian legal system remains fragmented and has not yet been able to provide maximum protection for victims of love scamming. The KUHP, UU ITE, UU TPKS, and other legal instruments address only certain aspects of this crime and were not designed to confront the complexity of emotionally based fraud in digital spaces. Comprehensive legal reform is required, encompassing the formulation of specific regulations, harmonization of cross-sectoral norms, strengthening of cybercrime units, enhancement of digital forensic capacities, integration of victim protection mechanisms, and expansion of international cooperation (Amriani,,& Rinaldi,2024). Without a holistic approach combining penal and non-penal measures, love scamming will continue to be a cybercrime that is difficult to eradicate and will persist in causing substantial harm to Indonesian society.

3. 2. Forms of Criminal Sanctions That May Be Imposed on Perpetrators of Love Scamming Based on the Applicable Legal Provisions in Indonesia

Arianto & Hidayat(2025) state victims of love scams are predominantly women and often experience depression, anxiety, and even suicidal tendencies as a result of the perpetrators' manipulative pressure (Niman & Rothhaar, 2023). In Indonesian positive law, this criminal act fulfills the elements of fraud as regulated in Article 378 of the Criminal Code (KUHP), namely unlawfully benefiting oneself or another person by using a false name, false status, deceit, or a series of lies. Love scam perpetrators who use false identities, stolen photographs, and fictitious emotional narratives clearly meet these elements and may therefore be punished with a maximum sentence of four years' imprisonment. In addition, the National Criminal Code (Law No. 1 of 2023) provides an additional legal basis through Article 492 concerning modern fraud based on identity falsification with a penalty of four years' imprisonment, as well as Article 495 concerning fraudulent acts causing economic loss with a penalty of one year's imprisonment, and even Article 483 regarding threats to disclose a victim's personal secrets.

More specifically, the handling of love scamming offenses in Indonesian criminal law still relies on general provisions on fraud as regulated in Article 378 of the Criminal Code. This article stipulates a maximum imprisonment of four years for perpetrators who employ deceit, use false names, or a series of lies to obtain unlawful gain. The provision was originally designed to address conventional fraud occurring through direct interaction. Article 378 of the Criminal Code emphasizes factual deception rather than emotional manipulation or digital identity misuse as found in love scamming. Consequently, from the outset, there are evident normative limitations in applying this article to fraud based on online relationships. In the context of the development of digital crime, the sanctions under Article 378 of the Criminal Code are often considered inadequate because they were not designed to address fraud involving electronic systems and online identity manipulation. Sibarani asserts that the maximum penalty of four years' imprisonment is too lenient for digital crimes that can cause substantial losses (Niman & Rothhaar, 2023). Marpaung adds that the modernization of fraud methods requires an update of criminal sanctions that are more proportional to the level of danger and the impact on victims (Marpaung,2018). These views reinforce the argument that, although formally applicable, the effectiveness of Article 378 in addressing love scamming remains limited.

Nevertheless, certain elements of Article 378 of the Criminal Code can still be used to prosecute love scamming perpetrators, particularly the elements of "deceit" and "a series of lies." Digital fraud continues to satisfy the element of deception even when committed through electronic platforms. Brenner also emphasizes that the manipulation of identity and information through digital devices still falls within the category of deceit in the framework of fraud (Brenner, S, 2010). However, applying this article to romance fraud requires extensive interpretation, because deception in love scamming is not limited to factual misrepresentation but also includes psychological exploitation that is difficult to measure using conventional fraud categories. The criminal sanctions stipulated in Article 378 of the Criminal Code are considered less relevant when compared to the impact of love scamming, which often involves substantial financial losses and profound emotional trauma. The average losses suffered by romance fraud victims reach tens to hundreds of millions of rupiah, figures far higher than those typically associated with conventional fraud. Whitty also notes that the psychological impact on romance fraud victims is far more severe because they experience a sense of personal betrayal (Whitty, 2018).

Accordingly, a four-year imprisonment penalty is viewed as disproportionate to the layered nature of love scamming offenses, both financially and emotionally.

A number of court cases indicate that Article 378 continues to be used to prosecute online fraud perpetrators, but it is often inadequate to address the complexity of love scamming. Judicial decisions in several online fraud cases show that judges tend to apply a combination of Article 378 of the Criminal Code and provisions of the Electronic Information and Transactions Law (UU ITE) to strengthen the criminal elements. Many fraud cases conducted through social media are proven using electronic transaction trails, yet Criminal Code provisions are often considered insufficiently flexible to accommodate technically complex digital evidence. This highlights the limitations of the Criminal Code in addressing modern fraud cases that exploit information technology.

The main obstacle in applying Article 378 of the Criminal Code in love scamming cases lies in proving the element of "deceit," which must be demonstrated concretely and in detail. Digital fraud is more difficult to prove because perpetrators can delete conversations, conceal traces, or use fake accounts. Cybercrime perpetrators often exploit international networks, cross-border infrastructure, and obfuscation technologies such as VPNs, making investigations more complex. This condition renders a Criminal Code oriented toward conventional evidence less compatible with dynamic, technology-based, and transnational crime patterns. Considering all these limitations, the use of Article 378 of the Criminal Code in addressing love scamming often serves only as an initial legal basis rather than a comprehensive solution. Sibarani (2020) emphasizes that the Criminal Code needs to be revised to accommodate the increasingly complex development of digital crime (Sibarani, 2020).

Because this crime is committed through electronic means, the Electronic Information and Transactions Law (UU ITE) constitutes the most relevant lex specialis. Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the UU ITE prohibits the dissemination of false or misleading information that causes consumer losses in electronic transactions, with a penalty of up to six years' imprisonment and a fine of one billion rupiah. This provision closely aligns with the pattern of love scamming, which exploits electronic messages, social media, and digital applications to deceive victims (Mulyani,2025). Furthermore, Article 35 in conjunction with Article 51 paragraph (1) of the UU ITE concerning the manipulation, creation, deletion, or alteration of electronic information carries a penalty of up to twelve years' imprisonment and a fine of up to twelve billion rupiah, and is highly relevant for prosecuting perpetrators who falsify photographs, identities, digital conversations, and fabricated emergency scenarios. If perpetrators engage in sextortion or content-based extortion, Article 27 paragraph (4) in conjunction with Article 45 paragraph (4) of the UU ITE may be applied, with a penalty of up to six years' imprisonment and a fine of one billion rupiah, as found in various forms of romance scams. Moreover, research by Mulyani shows that love scams often evolve into digital sexual violence, making the Sexual Violence Crimes Law (Law No. 12 of 2022) applicable in cases involving requests for intimate images, threats to disseminate content, or digital sexual exploitation (Mulyani, 2025).

Accordingly, the Electronic Information and Transactions Law is considered a more appropriate legal basis for prosecuting love scamming perpetrators because it specifically regulates unlawful acts committed through electronic media. According to Adi, the UU ITE provides a normative framework suited to the characteristics of digital crimes such as fraud conducted through messaging applications, social media, or online dating platforms (Adi,2021). Article 28 paragraph (1) of the UU ITE prohibits the dissemination of false information that causes consumer losses in electronic transactions, making it relevant in love scamming cases. Perpetrators frequently construct false narratives regarding identity, personal conditions, or emergency situations to deceive victims. The conveyance of false information lies at the core of romance fraud. Electronic messages containing falsehoods that cause losses can therefore be directly qualified as violations of Article 28 paragraph (1). Article 35 of the UU ITE regulates the prohibition of electronic identity falsification, which is a defining characteristic of love scamming. Perpetrators typically use fake photographs, fictitious identities, or stolen profiles to construct convincing online personas (Whitty & Garry, 2015). Digital identity falsification constitutes identity fraud that can cause significant harm to victims. Accordingly, Article 35 has direct relevance to the conduct of love scamming perpetrators who manipulate identity as part of their modus operandi. Article 51 of the UU ITE provides criminal sanctions for violations of Articles 28 and 35, with imprisonment of up to twelve years and fines of up to twelve billion rupiah. The criminal sanctions under the UU ITE are more severe than those under the Criminal Code because they were designed to regulate crimes that exploit information technology. The severity of these sanctions is necessary to create a deterrent effect against cybercrime perpetrators who often operate systematically and across borders. These penalties demonstrate the seriousness of the state in addressing digital fraud such as love scamming.

One advantage of the UU ITE over the Criminal Code is its capacity to cover acts committed entirely through digital networks. Digital crimes possess characteristics distinct from traditional crimes and therefore require appropriate regulation. The UU ITE explicitly covers the use of electronic systems, the dissemination of false information, and identity manipulation, thereby expanding the scope of criminal liability. According to

Adi, this regulation provides a stronger legal basis for addressing love scamming, where the entire sequence of acts is conducted online. However, the application of UU ITE sanctions is not without significant challenges, particularly with regard to digital evidence. In addition to evidentiary issues, another obstacle in applying the UU ITE is the transnational nature of love scamming, which creates jurisdictional difficulties. Therefore, although the UU ITE provides adequate norms, its enforcement depends on cross-jurisdictional coordination.

In a number of court decisions, the UU ITE has been used to strengthen legal action against digital fraud perpetrators. Law enforcement authorities often combine Articles 28 and 35 of the UU ITE with fraud provisions of the Criminal Code to reinforce evidentiary elements. Several online fraud cases have been successfully proven through digital conversation records, electronic transfer evidence, and device forensics. This demonstrates the effectiveness of the UU ITE in addressing crimes that exploit electronic communication. Based on all these findings, it can be concluded that love scamming perpetrators in Indonesia may be subject to the following forms of criminal sanctions: (1) fraud under Article 378 of the Criminal Code with a penalty of up to four years' imprisonment; (2) dissemination of false information causing consumer losses in electronic transactions under Article 28 paragraph (1) of the UU ITE with a penalty of up to six years' imprisonment; (3) falsification and manipulation of electronic information under Article 35 in conjunction with Article 51 paragraph (1) of the UU ITE with penalties of up to twelve years' imprisonment and multi-billion-rupiah fines; (4) electronic-based sexual crimes under the Sexual Violence Crimes Law if the perpetrator engages in digital harassment or sextortion; (5) additional criminal liability if elements of extortion, money laundering, or embezzlement are found; and (6) the application of modern fraud provisions under the National Criminal Code that strengthen the sentencing framework. All these legal instruments indicate that the Indonesian legal system has provided a fairly comprehensive sentencing framework, although it has not yet enacted specific regulations on love scams. Nevertheless, their effectiveness still requires increased law enforcement capacity, regulatory harmonization, and strengthened digital security infrastructure to ensure optimal public protection and a genuine deterrent effect for perpetrators

IV. CONCLUSIONS AND RECOMMENDATIONS

4.1 Conclusions

Based on the results of the study on the legal regulation and criminal sanctions for the crime of love scamming within the Indonesian legal system, several conclusions can be drawn as follows.

1. The legal regulation of love scamming in Indonesia remains fragmentary and has not been regulated as a specific offense. Its handling still relies on a combination of the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), the Sexual Violence Crimes Law (UU TPKS), the Personal Data Protection Law (UU PDP), and the Anti–Money Laundering Law (UU TPPU), which causes legal interpretation to depend heavily on law enforcement authorities and potentially leads to inconsistencies in practice.
2. The existing positive legal framework has not fully reflected the complexity of love scamming as a form of cybercrime that combines emotional manipulation, digital identity abuse, and economic loss. The Criminal Code and the National Criminal Code remain oriented toward conventional fraud, while the UU ITE and other regulations address only certain aspects, resulting in a regulatory framework that remains partial.
3. Normatively, criminal sanctions against love scamming perpetrators are relatively diverse, ranging from fraud and electronic identity falsification to digital sexual violence and money laundering. However, the effectiveness of sentencing has not been optimal due to challenges in digital evidence, limited capacity of law enforcement authorities, and the absence of specific sentencing standards for love scamming offenses.

4.2 Recommendations

The legal regulation of love scamming in Indonesia remains fragmentary and lacks a specific character, as it relies on a combination of the Criminal Code and various sectoral laws whose application depends on the interpretation of law enforcement authorities. The existing legal framework also does not yet reflect the complexity of love scamming as a cybercrime involving emotional manipulation and digital identity abuse. Although criminal sanctions are normatively available, the effectiveness of sentencing has not been optimal due to challenges in digital proof and the absence of specific sentencing standards.

REFERENCES

[1] Adi, R. (2021). *Hukum Siber dan Tantangan Penegakan Cybercrime di Indonesia*. Jakarta: Sinar Grafika.

[2] Amriani, N., & Rinaldi, K. (2024). Analisis Viktimologi Terhadap Kasus Love Scamming Pada Perempuan Korban Aplikasi Pencari Jodoh Online (Studi Kasus Perempuan Korban Aplikasi Pencari Jodoh Online). *Jurnal Sisi Lain Realita*, *09*(01).

[3] Arianto, V. A., & Hidayat, T. A. (2025). Penegakan Hukum Terhadap Tindak Pidana Love Scamming di Wilayah Hukum Kepolisian Daerah Sumatera Barat. *Jurnal Hukum Progresif*, *8*(9).

[4] Bimantari, N., Ayumeida Kusnadi, S., & Dwi Purwaningtyas, F. (2023). Perlindungan Hukum Bagi Korban Kejahatan Love Scam. *Jurnal Ilmu Hukum Wijaya Putra*, *1*(2).

[5] Brenner, S. (2010). *Cybercrime and the Law: Challenges, Issues, and Outcomes.* London: Routledge.

[6] Duha, A. (2024). Law for Ensuring Data Security in the Digital Age: Challenges for Government and Warnings for Us. *Verdict: Journal of Law Science*, *3*(2), 111–119. https://doi.org/10.59011/vjlaws.3.2.2024.111-119

[7] Duha, R. (2024). Punishment for Cybercrime: A Major Challenge in Modern Legal Systems. *Verdict: Journal of Law Science*, *3*(2), 86–93. https://doi.org/10.59011/vjlaws.3.2.2024.86-93

[8] Faber, P. (2024). The Frames of Romance Scamming. *Research in Language*, *22*(1), 1–23. https://doi.org/10.18778/1731-7533.22.1.01

[9] Kumalasari, N., Herwindya, S., & Wijaya, B. (2024). Persepsi Korban Love Scamming Di Media Sosial. *Jurnal Komunikasi Massa*, *17*(1), 45–59.

[10] Kumalasari, N., & Wijaya, S. H. B. (2024). *Manipulasi Informasi pada Korban Love Scamming di Media Sosial: Studi Kasus tentang Manipulasi Informasi pada Perempuan Korban Love Scamming di Kota Semarang*. Jurnal Komunikasi Massa, 17(2), 157–171.

[11] Maharani, B. A., Rahajeng, H. A., Triana, & Arianti, Z. D. (2025). Perlindungan Hukum Masyarakat dari Dampak Negatif Penggunaan AI. *Media Hukum Indonesia (MHI)*, *3*(2), 666–673. https://doi.org/10.5281/zenodo.15783168

[12] Marpaung, L. (2018). *Kejahatan Transnasional dan Tantangan Penegakan Hukumnya.* Jakarta: Kencana.

[13] Mulyani, M. (2025). Love Scam as a Manifestation of Online Gender-Based Violence: Aligning Legislation to Ensure Victim Protection. *Istinbath : Jurnal Hukum*, *22*(1), 247–256. https://doi.org/10.7334/psicothema2023.315

[14] Niman, S., Parulian, T. S., & Rothhaar, T. (2023). Online love fraud and the experiences of Indonesian women: a qualitative study. *International Journal of Public Health Science*, *12*(3), 1200–1208. https://doi.org/10.11591/ijphs.v12i3.22617

[15] PPATK. (2025). Buletin Statistik Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APUPPT) serta Pendanaan Proliferasi Senjata Pemusnah Massal (PPSPM). *Pusat Pelaporan Dan Analisis Transaksi Keuangan (PPATK)/ Indonesian Financial Transaction Reports and Analysis Center (INTRAC)*, *13*.

[16] Putri, N. K. D. S., & Saraswati, P. S. (2024). Perlindungan Hukum Terhadap Korban Modus Love Scam Dalam Situs Kencan Online di Indonesia. *Jurnal Mahasiswa Hukum Saraswati*, *04*(02).

[17] Qoir, M. N., & Ichsan, L. O. M. (2025). Non-Penal Policy in Combating Love Scamming. *Semarang State University Undegraduate Law and Society Review*, *5*(2).

[18] Rahardjo, S. (2021). *Cybercrime dan Penegakan Hukumnya di Indonesia*. Malang: UB Press.

[19] Retnowati, Y. (2015). Love Scammer: Komodifikasi Cinta dan Kesepian di Dunia Maya. *Jurnal Komunikologi*, *12*(2).

[20] Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1), 97–115. https://doi.org/10.17576/gema-2019-1901-06

[21] Sibarani, R. (2020). *Hukum Pidana Siber: Analisis atas Penipuan Elektronik.* Jakarta: Prenadamedia Group.

[22] Siregar, B. (2022). *Penegakan Hukum UU ITE dan Tantangan Pembuktian Digital.* Jakarta: Pustaka Yustisia.

[23] Sofiana, N., Purnomo, M., & Rosita, D. (2025). Analisis Yuridis Tindak Pidana Love Scamming Sebagai Kejahatan Siber. *Semarang Law Review (SLR)*, *6*(2).

[24] Solihin, R., & Zuhri, A. (2024). Criminal Liability of Love Scam Perpetrators in the Perspective of Positive Law and Islamic Criminal Law. *LEGAL BRIEF*, *13*(4), 1043–1051.

[25] Sultan, & Kursiswanti, E. T. (2024). Love Scamming dalam Jerat Hukum Pidana. *Jurnal Ilmu Hukum "THE JURIS," VIII*(2), 592–598.

[26] Temcharoenkit, S., & Rani, A. D. M. (2025). Strengthening Digital Citizens Against Love Scams: A Case Study of Indonesia and Thailand. *JUPSI: Jurnal Pendidikan Sosial Indonesia*, *3*(2), 107–116. https://doi.org/10.62238/jupsi.v3i2.276

[27] Whitty, M. T. (2017). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Journal of Cyberpsychology*, 10(3), 27–49.

[28] Whitty, M. T. (2018). The Psychology of Internet Fraud Victimisation. *Current Opinion in Psychology*, 19, 11–16.

[29] Whitty, M. T., & Buchanan, T. (2016). The Online Romance Scam: A New Crime for the 21st Century. *Cyberpsychology, Behavior, and Social Networking*, 19(5), 331–335.

[30] Whitty, M. T., & Garry, M. (2015). Scams and Online Deception. *Journal of Digital Crime*, 12(2), 112–127.