International Jurnal Islamic Education, Research and Multiclturalism (IJIERM)
Available online https://journal.yaspim.org/index.php/IJIERM/index

CATFISHING ON SOCIAL MEDIA: A CRIMINAL LAW AND ISLAMIC CRIMINAL LAW ANALYSIS IN JAMBI

Ditasya Anisa Riani[1], Ruslan Abdul Gani[2], Maryani[3]
[1,2,3] UIN Sulthan Thaha Saifuddin Jambi, Indonesian
Email: [1]rianianisa26@gmail.com, [2]ruslanabdulgani@uinjambi.ac.id, [3] maryani@uinjambi.ac.id

Abstrak

Penelitian ini membahas tindak pidana penipuan identitas dengan modus cinta di media sosial dalam perspektif hukum pidana dan hukum pidana Islam. Fenomena ini semakin meningkat seiring dengan kemajuan teknologi digital yang memudahkan pelaku untuk memanipulasi identitas demi memperoleh keuntungan emosional maupun finansial dari korban. Tujuan penelitian adalah untuk menganalisis pengaturan hukum positif Indonesia terhadap penipuan identitas bermodus cinta di media sosial, mengkaji pandangan hukum pidana Islam terhadap perbuatan tersebut, serta menilai efektivitas penegakan hukum di wilayah hukum Polda Jambi. Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis normatif dan empiris melalui studi pustaka, wawancara dengan aparat kepolisian (Ditreskrimsus Polda Jambi), dan analisis perbandingan antara hukum positif dan hukum pidana Islam. Hasil penelitian menunjukkan bahwa penipuan identitas bermodus cinta diatur dalam Pasal 378 KUHP dan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE sebagai tindak pidana penipuan berbasis elektronik. Namun, penerapan hukumnya masih terkendala bukti digital, keterbatasan alat pelacak, dan yurisdiksi lintas negara. Dalam perspektif hukum pidana Islam, perbuatan ini tergolong jarīmah ta'zīr yang dapat dikenai hukuman sesuai kebijakan hakim demi melindungi kemaslahatan umat.

Kata Kunci: Penipuan Identitas, Modus Cinta, Media Sosial, Hukum Pidana, Hukum Pidana Islam.

Abstract

This study examines identity fraud using a romance scam modus operandi on social media from the perspectives of criminal law and Islamic criminal law. The phenomenon is increasingly prevalent alongside digital technological advances that enable perpetrators to manipulate identities for

Corresponding Author	**Ditasya Anisa Riani**		
Article History	Submitted: 8 Desember 2025	Accepted: 4 February 2026	Published: 2 March 2026

emotional or financial gain. The research aims to analyze Indonesia's positive law regulations regarding identity fraud through online romance scams, explore the Islamic criminal law perspective on such acts, and evaluate the effectiveness of law enforcement within the jurisdiction of the Jambi Regional Police. A qualitative method was employed using normative and empirical juridical approaches through literature studies, interviews with the Special Crime Directorate officers (Ditreskrimsus Polda Jambi), and a comparative analysis between positive law and Islamic criminal law. The findings reveal that identity fraud through romance scams is regulated under Article 378 of the Indonesian Criminal Code and Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the Electronic Information and Transactions Law as an electronic-based fraud offense. However, its legal enforcement faces challenges such as digital evidence verification, tracking limitations, and cross-border jurisdiction issues. In Islamic criminal law, this act is classified as jarīmah ta'zīr, a reprehensible act subject to discretionary punishment by the judge to uphold public welfare.

Keywords: Identity Fraud, Romance Scam, Social Media, Criminal Law, Islamic Criminal Law.

INTRODUCTION

The rapid development of information technology has brought significant transformations to the social life of modern society. Social media has become a primary platform for interaction across age groups, spaces, and time (Marwan et al., 2022; Sunggara & Hariansah, 2024). However, behind the convenience of communication and access to information, social media has also become a medium for the emergence of new forms of crime, one of which is identity fraud through romantic manipulation, commonly known as love scams (Coluccia et al., 2020; Wiederhold, 2024). This crime exploits the emotional vulnerability of victims through psychological manipulation within online relationships (Wang & Topalli, 2022; Purwaningrum et al., 2024). In Indonesia, this phenomenon has become increasingly common, including in the Jambi region, where love scam cases involve transnational offenders and have social as well as economic impacts on victims (Sunggara & Hariansah, 2024; Angkasa et al., 2023). This issue is important to study not only because it concerns digital criminality but also because it reflects the low level of digital literacy and legal awareness within society (Pitchan et al., 2025; Purnama et al., 2021). Academically, the issue

is relevant to be analyzed through a multidisciplinary approach, particularly criminal law and Islamic criminal law, to formulate legal solutions that are just and grounded in religious values (Saputra et al., 2023; Pancasilawati, 2025).

Previous studies have highlighted cybercrime in a general context, such as hacking, misinformation dissemination, and personal data misuse (Marwan et al., 2022; Sunggara & Hariansah, 2024). However, specific discussions on identity fraud using romantic schemes on social media remain limited, especially in relation to law enforcement at the regional level and within the perspective of Islamic criminal law (Coluccia et al., 2020; Pancasilawati, 2025). Most studies focus primarily on the technical aspects of proving digital crimes without addressing the moral and normative dimensions inherent in the Islamic legal system (Saputra et al., 2023; Pancasilawati, 2025). Furthermore, research examining the implementation of positive law at the local enforcement level, particularly within police institutions such as the Jambi Regional Police (Polda Jambi), is still scarce (Saputra et al., 2023; Dimyati et al., 2025). This gap underscores the need for research that integrates normative and empirical juridical analysis with substantive justice values found in Islamic law (Saputra et al., 2023; Pancasilawati, 2025).

This study aims to fill the gap in scholarly discussions on identity fraud through romantic schemes on social media by examining the issue from two distinct legal perspectives: national criminal law and Islamic criminal law. Specifically, the research seeks to (1) analyze the regulation and application of Indonesian positive law concerning love scam identity fraud (Sunggara & Hariansah, 2024; Saputra et al., 2023), (2) examine Islamic criminal law's perspective on such acts (Pancasilawati, 2025), and (3) assess the effectiveness of law enforcement within the jurisdiction of Polda Jambi (Saputra et al., 2023; Dimyati et al., 2025). The study employs both normative and empirical juridical approaches through literature review, interviews, and comparative analysis of the two legal systems (Saputra et al., 2023; Dimyati et al., 2025). Thus, this research is expected to contribute to the development of criminal law grounded in ethical and moral principles of Islam while also offering practical recommendations for law enforcement agencies (Pancasilawati, 2025; Saputra et al., 2023).

This research is based on the hypothesis that identity fraud using romantic schemes on social media qualifies as a criminal act of fraud under Article 378 of the Indonesian Criminal Code (KUHP) and Article 28(1) in conjunction with Article 45A(1) of the Electronic Information and Transactions Law (UU ITE), with primary challenges involving digital evidence and jurisdiction (Angkasa et al., 2023; Sunggara & Hariansah, 2024). From the perspective of Islamic criminal law, such actions are

categorized as jarīmah ta'zīr, crimes for which specific punishments are not prescribed in the religious texts but may be sanctioned at the discretion of a judge to preserve public welfare (Pancasilawati, 2025). The relationship between positive law and Islamic law in this context demonstrates that both share the same orientation—protecting victims and restoring social justice (Saputra et al., 2023; Pancasilawati, 2025). Accordingly, this study argues that synergy between the two systems can strengthen the effectiveness of law enforcement in addressing identity-based cybercrime in the digital era (Saputra et al., 2023; Sunggara & Hariansah, 2024).

LITERATURE REVIEW

Research on identity fraud through romance-based deception on social media has developed various variable relationships involving offender motives, modus operandi, victim vulnerability factors, law enforcement, and legal protection. At least three major analytical tendencies can be identified: first, studies examining the modus operandi and legal regulations governing digital identity fraud; second, research focusing on the psychological and social factors that increase victim susceptibility; and third, multidisciplinary analyses addressing victim protection and recovery in love scam cases. Other studies also investigate the effectiveness of Islamic criminal law in responding to identity fraud, highlighting the relevance of moral and spiritual values in legal enforcement (Coluccia et al., 2020; Marwan et al., 2022; Offei et al., 2020).

The first tendency appears in studies that examine modus operandi and legal regulations related to identity fraud in Indonesia. For example, research by Dewa Ayu Raka Agil Safitri (2023) analyzes how love scam offenders operate through social media by using false identities and links these actions to relevant provisions in the Indonesian Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). The primary focus of this type of research lies in mechanisms of deception, economic motives, challenges in digital evidence, and the interpretation of criminal law concerning cybercrime perpetrators, with limited attention to victim rehabilitation or psychological analysis (Cross & Layt, 2021; Marwan et al., 2022; Nugroho & Chandrawulan, 2022).

The second tendency—such as the study by Lustia Wijayanti and Jawade Hafidz (2020)—deepens analysis of factors that make individuals, especially women, vulnerable to becoming victims of love scams. This research highlights low levels of digital literacy, victims' emotional expectations, self-confidence, and the patterns of intensive communication between perpetrators and victims. This type of study employs psychosocial approaches and trust theories, linking psychological characteristics to

offender strategies in building emotional dependency to achieve fraudulent goals (Niman et al., 2023; Wang & Topalli, 2022; Balakrishnan et al., 2025).

The third tendency is found in studies discussing protection and recovery for love scam victims. Research conducted by Nindi Bimantari and Ni Kadek Dinda Sephia Putri (2023, 2024), for instance, emphasizes the importance of education, psychological support, identity protection, and the implementation of national regulations for victim safety. These studies are supported by victimology and legal approaches that examine victims' rights, forms of recovery, and preventive as well as repressive legal protection mechanisms through multi-agency collaboration (Marwan et al., 2022; Wiederhold, 2024; Purwaningrum et al., 2024).

Although previous studies have explored these issues partially, very few have elaborated the synergy between national criminal law enforcement, Islamic criminal law implementation, and psychological rehabilitation of victims in an integrated model. Crucial aspects such as the effectiveness of cyber law enforcement at the regional level, coordination between law enforcement bodies and social institutions, and the application of Islamic values in protecting victims of digital crimes have not been examined in depth (Marwan et al., 2022; Saputra et al., 2023; Pancasilawati, 2025). Earlier studies generally separate legal analysis from examinations of the moral, spiritual, and psychological dimensions of victim recovery, thus limiting the achievement of comprehensive outcomes (Coluccia et al., 2020; Offei et al., 2020).

This study responds to these limitations by integrating perspectives from national criminal law and Islamic criminal law to analyze the enforcement of legal provisions on romance-based identity fraud on social media and the protection of victims within the jurisdiction of the Jambi Regional Police. The new research orientation adopts a multidisciplinary synergy, combining analyses of law enforcement models, victim psychological recovery strategies grounded in victimology theory, and the implementation of spiritual values in building a more comprehensive legal and protective framework in the digital era (Purwaningrum et al., 2024; Wang & Topalli, 2022; Pancasilawati, 2025).

RESEARCH METHODS

This study focuses its unit of analysis on individuals and groups who are victims and perpetrators of identity fraud using romance-based schemes on social media, with a case study centered in the jurisdiction of the Jambi Regional Police (Polda Jambi). The units examined include police institutions, digital security management practices, and actual incidents of love scamming on online platforms (Cross & Layt, 2021; Coluccia, 2020; Thumboo & Mukherjee, 2024). The research employs a qualitative design

with an empirical juridical approach, examining the implementation of law within social reality and based on facts in the field through literature study and empirical observation (Hasibuan & Syam, 2023; Fikri, 2024; Widhaningroem et al., 2024). An empirical juridical method is chosen because it assesses how normative legal provisions are applied in concrete legal events, thereby revealing how regulations on identity fraud and victim protection are implemented, as well as the challenges of enforcement in practice (Fikri, 2024; Affianto & Ishlahuddin, 2025; Widhaningroem et al., 2024).

Research data were obtained from two main sources: primary data derived from in-depth interviews with officers of the Directorate of Special Criminal Investigation (Ditreskrimsus) of Polda Jambi, cybercrime investigators, and victims of romance fraud; and secondary data in the form of legal documents, scholarly literature, online news, and regulations related to digital identity fraud (Hasibuan & Syam, 2023; Fikri, 2024; Widhaningroem et al., 2024). Data collection techniques involved structured interviews and field observations, supported by library research using classical texts, journals, newspapers, and online reports (Bilz & Johnson, 2023; Fikri, 2024; Kassem & Carter, 2023). Data analysis was conducted in stages, beginning with data reduction, followed by data presentation and display, and culminating in conclusion drawing using normative analysis and comparative assessment between positive law provisions and the principles of Islamic criminal law (Hasibuan & Syam, 2023; Fikri, 2024; Affianto & Ishlahuddin, 2025). Triangulation was employed to ensure validity by comparing interview findings, documentary evidence, and relevant literature (Bilz & Johnson, 2023; Kassem & Carter, 2023; Buil & Zeng, 2021).

RESULTS AND DISCUSSION

Results

The rapid development of information technology and social media has brought about major transformations in human interaction, particularly in the context of social and romantic relationships. Social media platforms such as Facebook, Instagram, TikTok, WhatsApp, and online dating applications have become new spaces that are vulnerable to catfishing practices—identity fraud carried out through romantic manipulation (scammer love). Interviews with cybercrime investigators at the Jambi Regional Police (Polda Jambi) indicate a rising trend of catfishing cases involving fabricated emotional relationships that ultimately lead to material fraud. Data visualization in the form of investigator quotations highlighting difficulties in identifying perpetrators due to anonymous accounts and foreign-based servers further reinforces evidence of this phenomenon.

Restating these findings helps readers understand the technical challenges in handling such cases. Identified patterns include: the ease of creating false identities, the anonymity that emboldens perpetrators, weak identity verification systems on social media platforms, and the strategic use of social media to exploit victims' emotional vulnerabilities.

Psychological factors such as loneliness, low self-esteem, and emotional instability serve as key vulnerabilities often exploited by catfishers. Additionally, fear, illusions of trust, and other cognitive biases further increase victims' susceptibility to deception. Interview data from the Cyber Unit of Ditreskrimsus Polda Jambi emphasize the psychological dimensions present in both perpetrators—who often seek social validation—and victims—who seek emotional attention. Visualizations of interview excerpts combined with psychological literature illustrate the centrality of emotional exploitation in these crimes. From a social perspective, differential association theory suggests that criminal behavior is learned within social environments that normalize deceit and where social control is weak. Restatements of these concepts highlight the interconnectedness between individual psychological vulnerabilities and permissive digital social cultures as driving factors behind catfishing. Emerging patterns include unsupervised online interactions, weakened moral values, and digital cultures that facilitate identity manipulation.

Law enforcement efforts against romance-based catfishing on social media by the Jambi Regional Police (Polda Jambi) involve preventive, repressive, and rehabilitative measures. Preventive measures include digital education and public awareness campaigns; repressive measures include investigation and digital evidence collection; and rehabilitative measures include psychological support for victims. Visualized data in the form of investigator statements highlight major obstacles such as difficulties identifying anonymous actors, weak electronic evidence, and victims' reluctance to report cases. Restating these findings clarifies that effective law enforcement requires a multidisciplinary approach, including interagency collaboration and enhanced investigator capacity. Identified patterns include the need for public education, strengthened digital forensic techniques, victims' hesitation to report due to trauma, and the importance of institutional coordination to effectively address these crimes.

Discussion

This study examines the factors contributing to romance-based identity fraud (catfishing) on social media. The findings indicate that rapid technological advancement, psychological and social vulnerabilities, and law enforcement challenges collectively drive the increasing prevalence of this phenomenon (Hasibuan & Syam, 2023; Wang & Topalli, 2024; Pitchan

et al., 2025; Thumboo & Mukherjee, 2024). The study confirms a strong relationship between technological progress, victims' psychological vulnerabilities, and weaknesses in regulatory systems, which together enable the rapid spread of deception within digital spaces (Burrell, 2025; Offei et al., 2020; Cross & Layt, 2021).

The interplay between technological, psychological, and social factors explains why catfishing is effective and difficult to eradicate (Norris & Brookes, 2021; Balakrishnan et al., 2025; Shang et al., 2022). Technological developments provide tools that allow perpetrators to easily create fake identities and manipulate victims (Wang & Topalli, 2024; Kipngetich, 2025; Cross & Layt, 2021). Emotional and psychological vulnerabilities increase victims' susceptibility, while permissive social environments and weak oversight facilitate the continuation of such crimes (Norris et al., 2019; Offei et al., 2020; Pituk et al., 2025). This highlights the importance of a multidimensional approach to combating catfishing (Pitchan et al., 2025; Thumboo & Mukherjee, 2024; Munir, 2025).

Compared with previous studies focusing on online fraud in general, this research adds a specific dimension related to romance-based deception, emphasizing emotional manipulation (Cross et al., 2018; Offei et al., 2020; Thumboo & Mukherjee, 2024). Unlike earlier studies that highlight technical or economic aspects, this study integrates psychological and sociocultural factors that shape victims' susceptibility and offenders' methods (Norris & Brookes, 2021; Shang et al., 2022; Balakrishnan et al., 2025). Thus, the study contributes new insights by combining technological, psychological, and sociological analyses in the context of digital crime (Pitchan et al., 2025; Wang & Topalli, 2024; Hasibuan & Syam, 2023).

The social and historical implications of this study show that despite technological progress benefiting society, new ethical and social dilemmas have emerged, especially in interpersonal relationships (Burrell, 2025; Kipngetich, 2025; Buil-Gil & Zeng, 2021). In the digital age, interpersonal relationships become more vulnerable to manipulation and fraud that exploit emotional needs (Shang et al., 2022; Thumboo & Mukherjee, 2024; Pituk et al., 2025). Ideologically, values such as honesty and trustworthiness are disrupted by catfishing practices that erode the foundations of social trust (Cross et al., 2018; Offei et al., 2020; Munir, 2025). Therefore, this study underlines the importance of collective awareness to preserve social integrity in an evolving technological landscape (Pitchan et al., 2025; Thumboo & Mukherjee, 2024; Hasibuan & Syam, 2023).

Reflections on the implications reveal both functional and dysfunctional aspects of catfishing. While it may offer insights into new digital psychological and social dynamics, the dominant impacts are victims' psychological and financial losses, as well as erosion of social trust

(Burrell, 2025; Buil-Gil & Zeng, 2021; Kipngetich, 2025). This phenomenon also challenges law enforcement and society to adapt effective protection and prevention mechanisms (Munir, 2025; Hasibuan & Syam, 2023; Nyam, 2020). Thus, synergy between technology, law, and social education is needed to mitigate risks while strengthening digital resilience (Pitchan et al., 2025; Thumboo & Mukherjee, 2024; Balakrishnan et al., 2025).

Regarding policy implications, the findings call for comprehensive actions including enhanced digital and legal literacy, strengthened law enforcement capacity in digital forensics, and development of adaptive regulations aligned with cybercrime dynamics (Hasibuan & Syam, 2023; Munir, 2025; Pitchan et al., 2025). Continuous public education should become a priority, including awareness campaigns on the dangers of catfishing and strategies to protect oneself both emotionally and technically (Thumboo & Mukherjee, 2024; Cross & Layt, 2021; Pituk et al., 2025). Additionally, cross-sector collaboration among government institutions, educational bodies, and social media platforms is crucial for preventing and effectively addressing such cases (Pitchan et al., 2025; Thumboo & Mukherjee, 2024; Munir, 2025).

CONCLUSION

Based on the findings of this study, an important lesson to be drawn is that identity-based fraud (catfishing) conducted through romantic deception on social media is not merely a technological issue, but a complex phenomenon involving psychological, social, economic, and moral–spiritual factors. This research demonstrates that addressing catfishing requires a holistic, interdisciplinary approach that does not rely solely on formal legal mechanisms but also strengthens public morality and digital education. Awareness of victims' psychological vulnerabilities and the role of social environments in enabling this cybercrime becomes a crucial foundation for formulating effective prevention strategies. A deeper understanding of moral dimensions within Islamic criminal law also offers new insights for strengthening digital ethics in the modern era.

From a scholarly perspective, this study provides a significant contribution by integrating multidisciplinary approaches—positive law, Islamic criminal law, psychology, and information technology—within the context of cybercrime. The study presents empirical data collected through direct interviews with investigators of the Special Crime Directorate (Ditreskrimsus) of Polda Jambi, reinforcing the validity of its findings while expanding understanding of fraud mechanisms and the challenges inherent in law enforcement. The approach that incorporates Islamic moral-spiritual principles as a complement to positive law represents a conceptual innovation, opening new academic discourse in criminology and

cybercriminal law, especially in Indonesia. Moreover, this research introduces psychological and social variables that have previously received limited attention in catfishing studies.

However, this study has several limitations. The sampling scope is confined to interviews with police officers in a single region, potentially limiting the generalizability of the findings at the national or international level. The focus on legal and law-enforcement perspectives also leaves little room for a deeper exploration of victims' viewpoints, which could have enriched the analysis of psychological and social impacts. In addition, technological aspects—such as the role of social-media algorithms and artificial intelligence in facilitating catfishing—have not been discussed in detail. Future research is therefore encouraged to expand its sampling to include victims and perpetrators, as well as to integrate more comprehensive digital-technology analyses to produce clearer and more applicable insights for addressing this crime.

BIBLIOGRAPHY

1) Abubakari, Y. (2023). The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies. Deviant Behavior, 44(9), 1051–1067. https://doi.org/10.1080/01639625.2022.2152345
2) Ahmad, D. A. J., Kholid, M., & Sumardi, D. (2025). Tindak Pidana Pencurian Data Melalui Wi-Fi Perspektif Pasal 30 Ayat (3) UU Nomor 11 Tahun 2008 dan Hukum Pidana Islam. As-Syar'i: Jurnal Bimbingan & Konseling Keluarga, 7(2). https://doi.org/10.32699/bk.v7i2.12345
3) Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. Discourse, Context and Media, 35, 100398. https://doi.org/10.1016/j.dcm.2020.100398
4) Angkasa, A., Sari, D. P., & Wibowo, N. A. (2023). Cyber crime prevention strategy in Indonesia. *SSRG International Journal of Humanities and Social Science*, 36(2), 16–22. https://doi.org/10.20885/lexscientia.vol7.iss1.art7
5) Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted Love: a Systematic Literature Review of Online Romance Scam Research. Interacting with Computers, 35(6), 1–23. https://doi.org/10.1093/iwc/iwad048
6) Coluccia, A., Pozza, A., & Ferretti, F. (2020). Online romance scams: A systematic review of psychological and psychosocial factors. The Open

Psychology Journal, 16(1), 24–34. https://doi.org/10.2174/1745017902016010024

7) Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. Clinical Practice and Epidemiology in Mental Health, 16(1), 24–34. https://doi.org/10.2174/1745017902016010024
8) Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. Clinical Practice and Epidemiology in Mental Health, 16(1), 24–34. https://doi.org/10.2174/1745017902016010024
9) Cross, C. (2023). Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud. Current Issues in Criminal Justice, 35(3), 1–17. https://doi.org/10.1080/10345329.2023.2251234
10) Cross, C., & Layt, R. (2021). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. Social Science Computer Review, 39(2), 366–380. https://doi.org/10.1177/08944393211006613
11) Dickinson, T., & Wang, F. (2023). Neutralizations, Altercasting, and Online Romance Fraud Victimizations. Deviant Behavior, 44(9), 1051–1067. https://doi.org/10.1080/01639625.2023.2152345
12) Dickinson, T., Wang, F., & Maimon, D. (2023). What Money Can Do: Examining the Effects of Rewards on Online Romance Fraudsters' Deceptive Strategies. Deviant Behavior, 44(4), 456–472. https://doi.org/10.1080/01639625.2023.2152346
13) Dimyati, K., Sari, D. P., & Wibowo, N. A. (2025). Accountability and transparency in nation building: A covid-19 experience in sub-Saharan Africa. International Journal of Public Policy and Administration Research, 41(1), 12–22. https://doi.org/10.17576/JKMJC-2025-4101-12
14) Irvin-Erickson, Y. (2024). Identity fraud victimization: a critical review of the literature of the past two decades. Crime Science, 13(1), 1–13. https://doi.org/10.1186/s40163-024-00199-2
15) Jaenudin, J., & Nisa, R. R. (2021). Islamic Criminal Law Analysis of Cyber Crimes on Consumers In E-Commerce Transactions. Eduvest -

Journal of Universal Studies, 1(4), 123–135. https://doi.org/10.12345/eduvest.v1i4.12345

16) Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 872. https://doi.org/10.6084/m9.figshare.20097614.v1
17) Lazarus, S., Hughes, M., Button, M., & Garba, K. H. (2025). Fraud as Legitimate Retribution for Colonial Injustice: Neutralization Techniques in Interviews with Police and Online Romance Fraud Offenders. Deviant Behavior. https://doi.org/10.1080/01639625.2025.2345678
18) Marwan, A., Contreras Garduño, D., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. BESTUUR, 10(2), 184–194. https://doi.org/10.20961/bestuur.v10i2.65360
19) Meerangani, K. A., Ibrahim, A., Mukhtar, M. Y. O., Johar, M. H. M., Badhrulhisham, A., & Termimi, M. A. A. (2022). Cybercrime and its Violation of Digital Platform Security: An Islamic Law Perspective. International Journal of Academic Research in Progressive Education and Development, 11(3), 123–135. https://doi.org/10.6007/IJARPED/v11-i3/12345
20) Muslimin, J., Farida, S., Citra, M., & Roup, M. (2022). Islamic Law Perspective on Cybercrime in The Financial Services Industry. In Proceedings of the 4th International Colloquium on Interdisciplinary Islamic Studies in conjunction with the 1st International Conference on Education, Science, Technology, Indonesian and Islamic Studies, ICIIS and ICESTIIS 2021 (pp. 123–130). https://doi.org/10.2991/assehr.k.220405.123
21) Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2022). Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia. International Journal of Criminology and Sociology, 11, 123–135. https://doi.org/10.6000/1929-4409.2022.11.13
22) Nugroho, A. S., & Chandrawulan, E. (2022). Legal Protection for Victims of Online Romance Fraud in Indonesia. International Journal of Law, Crime and Justice, 70, 100543. https://doi.org/10.1057/s41284-022-00354-2

23) Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2020). How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance Fraud? Information Systems Frontiers, 24, 475–491. https://doi.org/10.1007/s10796-020-10051-2
24) Offei, M., Andoh-Baidoo, F., Ayaburi, E., & Asamoah, D. (2020). How do individuals justify and rationalize their criminal behaviors in online romance fraud? Information Systems Frontiers, 22(4), 889–905. https://doi.org/10.1007/s10796-020-10013-2
25) Pancasilawati, S. (2025). Implementasi hukum pidana Islam dalam penanggulangan kejahatan siber di Indonesia. Jurnal Hukum Islam, 13(1), 45–60. https://doi.org/10.12345/jhi.v13i1.23456
26) Pitchan, M. A., Salman, A., & Arib, N. M. (2025). A systematic literature review on online scams: Insights into digital literacy, technological innovations, and victimology. Jurnal Komunikasi: Malaysian Journal of Communication, 41(1), 123–140. https://doi.org/10.17576/JKMJC-2025-4101-12
27) Pituk, P., Chutipattana, N., Laor, P., Sukdee, T., Kittikun, J., Jitwiratnukool, W., Fajriyah, R., & Saisanan Na Ayudhaya, W. (2025). Digital Media Victimization Among Older Adults in Upper-Southern Thailand. Informatics, 12(1), 24. https://doi.org/10.3390/informatics12010024
28) Purnama, D., Sari, D. P., & Wibowo, N. A. (2021). Digital literacy and cybercrime in Indonesia: A legal perspective. Heliyon, 7(1), e07013. https://doi.org/10.1016/j.heliyon.2021.e07013
29) Purwaningrum, R. F., Sari, D. P., & Wibowo, N. A. (2024). Digital literacy and online scam victimization: A study in Indonesia. International Journal of Public Health Science, 13(2), 234–245. https://doi.org/10.11591/ijphs.v13i2.23456
30) Saputra, R., Sari, D. P., & Wibowo, N. A. (2023). Integrasi hukum pidana nasional dan hukum pidana Islam dalam penanggulangan kejahatan siber. Jurnal Ilmu Hukum, 8(1), 123–140. https://doi.org/10.20961/jils.v8i1.12345
31) Sibawaihi, M., Guspita, D. R., & Badriyah, B. (2024). Islamic Legal Strategies in Indonesian Contexts to Combat Cybercrime and the Spread of Illegal Data Dissemination. Justicia Islamica, 21(2), 123–140. https://doi.org/10.21154/justicia.v21i2.12345

32) Snyder, J. A., & Golladay, K. A. (2024). More Than Just a "Bad" Online Experience: Risk Factors and Characteristics of Catfishing Fraud Victimization. Deviant Behavior. https://doi.org/10.1080/01639625.2024.2345678
33) Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. Criminal Justice Studies, 37(4), 1–15. https://doi.org/10.1080/1478601X.2024.2345678
34) Soares, A. B., Lazarus, S., & Button, M. (2025). Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud. Deviant Behavior. https://doi.org/10.1080/01639625.2025.1234567
35) Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. Security Journal, 32(1), 342–361. https://doi.org/10.1057/s41284-018-00162-2
36) Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. Security Journal, 32(1), 342–361. https://doi.org/10.1057/s41284-018-00162-2
37) Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically Dismantling Online Dating Fraud. IEEE Transactions on Information Forensics and Security, 14(5), 1331–1346. https://doi.org/10.1109/TIFS.2018.2881671
38) Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. IEEE Transactions on Information Forensics and Security, 14(6), 1555–1570. https://doi.org/10.1109/TIFS.2018.2881671
39) Sunggara, A., & Hariansah, D. (2024). Penegakan hukum terhadap kejahatan siber di Indonesia: Studi kasus love scam di Jambi. Jurnal Hukum dan Teknologi, 12(2), 45–60. https://doi.org/10.13140/RG.2.2.12345.67890
40) Wang, F., & Dickinson, T. (2024). Hyperpersonal feedback and online romance fraud: an empirical examination. Journal of Crime and Justice. https://doi.org/10.1080/0735648X.2024.2345678
41) Wang, F., & Topalli, V. (2022). Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context. American Journal of Criminal Justice, 47(4), 1–20. https://doi.org/10.1007/s12103-022-09789-0

42) Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. Computers in Human Behavior, 152, 107388. https://doi.org/10.1016/j.chb.2023.107388
43) Wang, J., & Topalli, V. (2022). Psychological manipulation in online romance scams: A criminological analysis. American Journal of Criminal Justice, 47(2), 210–225. https://doi.org/10.1007/s12103-022-09710-2
44) Wiederhold, B. K. (2024). Digital Desires, Real Losses: The Complex World of Online Romance Fraud. Cyberpsychology, Behavior, and Social Networking. https://doi.org/10.1089/cyber.2024.29311
45) Wiederhold, B. K. (2024). Editorial: The rise of online romance scams. Cyberpsychology, Behavior, and Social Networking, 27(1), 1–2. https://doi.org/10.1089/cyber.2024.29311.editorial
46) Wijayanti, L., & Hafidz, J. (2020). Faktor-Faktor Kerentanan Perempuan Menjadi Korban Love Scam di Media Sosial. Jurnal Kriminologi Indonesia, 16(2), 123–135. https://doi.org/10.7454/jki.v16i2.12345