The 7th Open Society Conference (OSC) 2025
Faculty of Law, Social and Political Science
Universitas Terbuka
DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

Legal Protection for Online Fraud Victims in the Context of Inclusive Digital Transformation in Indonesia

Eka Wahyu Octaviana
Law Program, Faculty of Law, Social and Political Science, Universitas Terbuka, Indonesia
e-mail: 052891385@ecampus.ut.ac.id

Abstract

This study analyzes the legal protection framework for online fraud victims amidst the rapid digital transformation in Indonesia. Although digital development has fostered inclusive economic growth, it has also increased the public's vulnerability to cybercrime. This research finds that the existing legal framework, namely the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), remains partial and ineffective in ensuring the restoration of victims' rights. The current regulations primarily focus on criminal aspects and sanctions for perpetrators, while the mechanism for restitution or compensation for victims is often unclear and difficult to access. This research employs a normative legal research method with a descriptive-analytical approach, applying both a statute approach and a conceptual approach. Primary and secondary legal materials were analyzed qualitatively to identify legal gaps and formulate an ideal protection model. The analysis results show that victims face significant challenges in accessing justice, including difficulties in collecting evidence and tracing perpetrators, the limited capacity of law enforcement officials, and a lack of public digital literacy. To address these issues, this article proposes a multidimensional solution. First, regulatory reforms are needed to focus on victims' rights and establish a more explicit duty of care for digital service providers. Second, enhancing the capacity of law enforcement in digital forensics and inter-agency collaboration is essential. Third, a stronger collaboration among the government, the private sector, and the public is required to build an integrated case reporting and handling system. Finally, inclusive digital transformation, supported by massive digital literacy campaigns, must serve as a fundamental foundation for creating a safe and equitable digital space for all citizens.

Keywords: *cybercrime victims, inclusive digital transformation, legal gap, legal protection, online fraud, restitution.*

INTRODUCTION

The rapid pace of digital transformation in Indonesia has brought numerous conveniences and fostered inclusive economic growth. However, this progress has also opened the door to a rise in cybercrime, particularly online fraud. Various schemes, from phishing and e-commerce scams to illegal digital investments, have caused significant financial losses and eroded public trust in the digital ecosystem [1]. This presents an ironic situation: while the government promotes digitalization, vulnerable segments of society are becoming victims of crimes that exploit this very technology. Thus, the issue of legal protection for online fraud victims is of paramount importance.

This is not a new issue in academic discourse. Several previous studies have examined legal protection for cybercrime victims, highlighting the challenges in implementing existing regulations. For instance, Hidayat (2018) highlighted the obstacles law enforcement faces in

DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

prosecuting online fraud perpetrators who use anonymous identities [2]. Additionally, Santoso (2020) underscored the lack of an effective mechanism for restitution, or the recovery of losses, for victims [3]. However, most of these studies tend to focus on analyzing existing regulations without comprehensively linking them to the specific challenges of inclusive digital transformation, where public digital literacy is varied and access to justice is often limited.

Despite the legal foundation provided by Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) and the Criminal Code (KUHP), a significant legal gap persists. This gap is evident in several areas: (1) the absence of specific regulations that mandate digital platforms to be fully responsible for preventing and combating fraud; (2) minimal clear provisions for an easily accessible and effective restitution mechanism for victims; (3) difficulties in providing evidence and establishing jurisdiction, which frequently impede legal proceedings; (4). This ambiguity leaves victims in a powerless position, facing a lengthy and often fruitless legal process.

To address these problems, this article proposes a comprehensive and multidimensional solution. First, regulatory reforms are needed that not only focus on criminal penalties but also on victim protection, including establishing more explicit obligations for digital service providers. Second, enhancing the capacity of law enforcement in digital forensics and improving inter-agency coordination are essential to speed up investigations. Third, collaboration among the government, the private sector (digital platforms and banks), and civil society must be strengthened to build an integrated system for reporting and handling cases. Finally, digital literacy must be continuously promoted as a preventive measure to equip the public with a strong understanding of how to avoid online fraud traps.

METHOD

This study employs a normative legal research method with a descriptive-analytical approach. This method was chosen because its focus is on positive legal norms, legal principles, and doctrines relevant to the issue of legal protection for online fraud victims [4]. The descriptive-analytical approach is used to thoroughly analyze and describe how existing laws and regulations, such as the UU ITE, KUHP, and other related rules, govern the protection of online fraud victims.

The study also utilizes a statistical approach and a conceptual approach [5]. The statute approach is used to comprehensively examine all laws and regulations related to cybercrime and victim protection to identify any existing legal gaps. Meanwhile, the conceptual approach is used to analyze legal concepts such as legal protection, justice, and legal responsibility in the context of cybercrime, in order to formulate an ideal model of legal protection.

The legal materials used include primary and secondary sources. Primary legal materials consist of relevant laws and regulations, such as the UU ITE, KUHP, and related court decisions. Secondary legal materials are sourced from legal literature, academic journals, research findings, books, and articles on similar issues from the last 10 years (2015-2025). All collected materials are then analyzed using qualitative analysis techniques, which involve interpreting, classifying, and systematizing data to find logical patterns, relationships, and conclusions [6]. The results of this analysis are expected to provide conceptual recommendations for more effective policy and law enforcement reforms.

DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

RESULT AND DISCUSSION

1. The Legal Framework for Comprehensive Protection of Online Fraud Victims

The current legal framework for protecting online fraud victims in Indonesia is partial and not yet comprehensively integrated. While the UU ITE serves as the primary legal basis, this regulation focuses more on criminal aspects and sanctions for perpetrators, as stipulated in Article 28(1) and Article 35(3). These articles are not specific enough in regulating the mechanism for restoring victims' rights, especially concerning restitution or compensation. As a result, victims often have to navigate a lengthy and complex civil legal path to recover their financial losses.

In addition to the UU ITE, the Criminal Code (KUHP) is often used through its fraud article (Article 378). However, applying this article to cybercrime faces challenges, particularly in providing evidence, as digital evidence is easily manipulated (2). Furthermore, the UU ITE and KUHP are not synergistically integrated due to their differing focuses. Similarly, the Consumer Protection Law is not relevant in cases of online fraud involving fake or anonymous identities.

In practice, many studies find that victims remain in a vulnerable position. The UU ITE does not explicitly guarantee the right to restitution; compensation is only seen as an option, not a legal obligation. As a result, protection tends to focus on the criminal prosecution of the perpetrator without ensuring financial and moral recovery for the victim. It is necessary to expand the status of "victim" in the UU ITE beyond just "formal consumers" to include victims of broader digital fraud, such as illegal investments or *love scams*.

The lack of a specific and integrated legal umbrella creates legal uncertainty for victims. To date, there is no single regulation that specifically and comprehensively governs the protection of cybercrime victims [1]. This is compounded by the absence of a dedicated institution to manage complaints and facilitate prompt recovery. Therefore, even with a criminal legal framework in place, the protection of victims' rights, especially their right to recovery, is still weak and ineffective in ensuring justice.

2. Challenges for Online Fraud Victims in Accessing Justice Amid Rapid Digital Transformation

Online fraud victims in Indonesia face significant challenges in obtaining restitution and justice through legal channels. A primary obstacle is the difficulty of proving and tracing perpetrators [2]. Cybercriminals often use fake identities, anonymous IP addresses, and various techniques to conceal their digital footprints. This makes police investigations complicated, time-consuming, and often fruitless. Consequently, victims feel hopeless and are unwilling to pursue a legal process they believe is not worth the time and cost.

Furthermore, the lack of an effective restitution mechanism is a major challenge. Although criminal law allows for compensation, the process is not integrated into a single system. Victims typically have to file a separate civil lawsuit after a criminal verdict is final, which requires additional costs, time, and effort [3]. This is worsened by the difficulty of executing civil judgments, especially if the perpetrator has no assets or is outside Indonesian jurisdiction. As a result, victims often only achieve a "victory on paper" without any real financial recovery.

Other challenges include the low digital literacy of the public and the unclear role of digital platforms [1]. Many victims do not know how to secure digital evidence or report cases correctly. Meanwhile, digital platforms like marketplaces or social media often remain passive, providing only a report feature without a proactive mechanism to verify user identities or take responsibility

DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

for resulting losses. This creates a vicious cycle where victims receive inadequate help from both law enforcement and private entities, making the pursuit of justice increasingly difficult.

Overall, Indonesia's legal system faces fundamental challenges: weak and limited regulations, low capacity of law enforcement, and under-empowered victims. The lack of public awareness of victims' rights and the disparity in restitution application among courts also worsen the situation. As a result, many restitution requests are rejected or not processed consistently, and online fraud victims often fail to achieve material and moral recovery.

3. Implementing Inclusive Digital Transformation to Reduce Online Fraud Risks

Inclusive digital transformation is a key strategy to mitigate the risks of online fraud, particularly for protecting vulnerable groups. Effective implementation focuses not only on providing technological infrastructure but also on building digital literacy and strengthening the cybersecurity ecosystem. The low level of digital literacy among the elderly and rural communities, for instance, makes them prime targets for phishing and social engineering [7]. Therefore, proactive policies are needed to close this gap.

The inclusive digital transformation strategy has two main dimensions. The first is digital education and literacy. Education programs specifically designed for vulnerable groups, with easy-to-understand materials, have proven effective in increasing public awareness of cyber threats [8]. This helps them identify and avoid fraud. The second is regulation and multi-stakeholder collaboration. A strong regulatory framework is needed to ensure that digital platforms and financial institutions are responsible for protecting their users. This must include obligations to provide robust verification mechanisms, easily accessible reporting systems, and a rapid response to fraud reports.

Legal protection alone is insufficient without a strong and widespread preventive security system. Inclusive digital transformation provides a foundation for more effective legal protection, as a digitally literate public and a secure ecosystem can significantly reduce the risk of fraud [F10]. Furthermore, this transformation should leverage advanced technologies like Artificial Intelligence (AI) to detect identity fraud and deepfakes [9]. This integration of education, technology, and regulation is the most effective formula for creating a safe and inclusive digital space for all Indonesian citizens.

4. Roles and Responsibilities of Stakeholders in Preventing and Handling Online Fraud

The effectiveness of protecting online fraud victims depends heavily on the integrated synergy and responsibilities of various parties, not just the government. Based on analysis, these crucial roles are divided among the government, digital platforms, financial institutions, and the public.

As a regulator, the government has a fundamental responsibility to create a strong and adaptive legal framework [9]. Its strategic role includes drafting regulations, overseeing digital platforms, and conducting public education. The Ministry of Communication and Digitalization (Komdigi), for example, has implemented the SAMAN mechanism to enforce compliance among electronic system providers and impose administrative sanctions for non-compliance. Similarly, the Financial Services Authority (OJK) actively protects consumers by raising awareness of legal versus illegal markets, imposing strict sanctions under the P2SK Law (2023), and providing complaint services for illegal fintech entities.

DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

Digital platforms and financial institutions act as the first line of defense. Platforms, such as e-commerce sites and social media, are responsible for implementing safety-by-design principles, content moderation, and strict verification mechanisms [10]. Studies show that platforms that are proactive in deleting fake accounts have a lower incidence of fraud. Likewise, financial institutions, including banks and fintech companies, are responsible for strengthening transaction security, educating customers on data confidentiality, and providing efficient channels to block fraudulent accounts and recover funds.

Finally, the public's role cannot be overlooked. Citizens must be smart and vigilant digital users. Widespread digital and financial literacy is a fundamental requirement, as demonstrated by various community programs that have successfully increased awareness of phishing and other fraud schemes [11] [12]. A critical attitude toward information and proactive reporting of fraud to authorities or platforms is essential. Data show that active collaboration between the public and law enforcement can accelerate investigations and the arrest of perpetrators [13]. Therefore, comprehensive legal protection can only be achieved through an integrated ecosystem where each party fulfills its role optimally. This integration is the foundation for an inclusive digital transformation that not only drives economic growth but also ensures security for all users.

5. Policy Recommendations to Strengthen Legal Protection for Online Fraud Victims

Formulating effective policy recommendations to strengthen legal protection for online fraud victims requires a holistic approach encompassing prevention, law enforcement, and education. The analysis shows that the most strategic policies must be integrated and adaptive. In prevention, policies should foster collaboration between the government and the private sector, especially technology companies and financial institutions, to develop stronger early detection and identity verification systems [14]. For example, the government could require digital platforms to implement multi-factor authentication and proactively monitor suspicious activities.

Next, to strengthen law enforcement, a crucial first step is to fortify the national legal framework. As of now, Indonesia lacks a specific law governing online fraud, relying instead on the UU ITE and OJK consumer protection regulations. This has resulted in policies that are not firm enough to restore victims' rights and deter perpetrators [15] [16]. Therefore, a specific law or regulation is needed to clarify provisions for restitution (*restorative justice*), make restitution a mandatory additional penalty, and establish a swift mechanism for victim recovery. Additionally, law enforcement officials need enhanced digital forensics capacity. Technical limitations, as reported in North Sumatra police departments, often hinder perpetrator identification [17] [18]. Policy recommendations include creating a special digital task force within the police, strengthening cross-agency cooperation (e.g., Kominfo, BSSN, and OJK), and establishing a more systematic virtual police mechanism to respond to public reports before they escalate to formal legal proceedings.

CONCLUSION

Indonesia's rapid digital transformation has created immense opportunities but has also increased the public's vulnerability to online fraud. This study concludes that the existing legal protection framework for digital fraud victims is partial and fails to fully guarantee the restoration of their rights. The UU ITE and KUHP primarily focus on the criminal aspects of perpetrators, while providing minimal certainty for victim restitution and compensation. The challenges of

DOI: 10.33830/osc.v3i1.7039 / ISSN: 3032-2227

evidence, cross-border jurisdiction, and low digital literacy further worsen victims' ability to access justice.

This research asserts that effective legal protection requires a multidimensional approach: regulatory reform that prioritizes victim rights, enhanced law enforcement capacity in digital forensics, and active involvement from the private sector. Furthermore, an inclusive digital transformation must be the foundation, with an emphasis on digital literacy education and strengthening system security as integral parts of the protection strategy. The integration of legal frameworks, technology, education, and multi-stakeholder collaboration is the key to building a fair, effective, and sustainable system for protecting online fraud victims.

REFERENCES

[1] S. Wahyudi, "Dampak Penipuan Online terhadap Kepercayaan Publik di Era Digital," *Jurnal Komunikasi dan Media*, vol. 5, no. 1, pp. 45–58, 2021.
[2] R. Hidayat, "Kendala Penegakan Hukum Terhadap Pelaku Penipuan Online di Indonesia," *Jurnal Hukum dan Pembangunan*, vol. 48, no. 2, pp. 221–236, 2018.
[3] B. Santoso, "Analisis Yuridis Terhadap Perlindungan Korban Kejahatan Siber di Indonesia," *Journal of Law Review*, vol. 20, no. 1, pp. 1–15, 2020.
[4] P. M. Marzuki, *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2021.
[5] S. Soekanto and S. Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: PT Raja Grafindo Persada, 2015.
[6] L. J. Moleong, *Metodologi Penelitian Kualitatif*. Bandung: PT Remaja Rosdakarya, 2018.
[7] S. Soekanto and S. Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: PT Raja Grafindo Persada, 2015.
[8] R. Rudiyanto, "Peran lembaga keuangan dalam mencegah jeratan pinjaman online ilegal," *Jurnal Ekonomi Manajemen Akuntansi Keuangan Bisnis Digital*, vol. 4, no. 1, pp. 229–240, 2025.
[9] C. J. Zhang, A. Q. Gill, B. Liu, and M. J. Anwar, "AI-based Identity Fraud Detection: A Systematic Review," 2025.
[10] A. Gunawan and S. Hadi, "Peran Platform E-commerce dalam Mencegah dan Menangani Kasus Penipuan Online di Indonesia," *Jurnal Hukum Bisnis*, vol. 15, no. 2, pp. 89–104, 2021.
[11] K. Nisa, P. Purwono, O. P. Handayani, and S. Setiawan, "Peningkatan literasi digital: Edukasi kejahatan siber dan pinjaman online ilegal MAN 2 Cilacap," *Jurnal Pengabdian Masyarakat – PIMAS*, vol. 4, no. 2, pp. 1–15, 2024.
[12] S. Andaiyani, Yunisvita, T. Yunisvita, and M. Pratiwi, "Optimalisasi peran perguruan tinggi: Pentingnya literasi keuangan digital dalam mencegah cybercrime," *Sricommerce: Journal of Sriwijaya Community Services*, vol. 4, no. 2, pp. 45–60, 2023.
[13] B. Setiawan and T. Mulyana, "Partisipasi Masyarakat dalam Upaya Mitigasi Kejahatan Online Melalui Pelaporan Aktif," *Jurnal Kriminologi Indonesia*, vol. 18, no. 1, pp. 1–15, 2022.
[14] M. F. Sanusi and Ariyanti, "Perlindungan hukum terhadap korban tindak pidana penipuan yang dilakukan oleh pelaku usaha e-commerce berbasis transaksi elektronik," *Merdeka Law Journal*, vol. 5, no. 2, pp. 171–178, 2025.
[15] A. R. Hendrawan et al., "Perlindungan hukum bagi korban kejahatan digital dalam perspektif UU ITE dan KUHP," *Causa: Jurnal Hukum dan Kewarganegaraan*, vol. 14, no. 12, pp. 71–80, 2025.
[16] F. P. Maharani, "Perlindungan hukum terhadap korban penipuan online investasi ilegal menurut UU ITE (UU No.19/2016)," *Lex Privatum*, vol. 13, no. 4, 2024.
[17] L. Ekayani and H. Djanggih, "Perlindungan hukum nasabah terhadap kejahatan pencurian data pribadi (phishing) di lingkungan perbankan," *Journal of Philosophy (JLP)*, vol. 4, pp. 22–40, 2023.
[18] A. H. Samudra, "Redressing the online transaction fraud victim treatment and interest fulfillment in the criminal justice system," *Jurnal Hukum & Pembangunan*, vol. 49, no. 3, pp. 650–656, 2019.