# LEGAL PROTECTION FOR VICTIMS OF IDENTITY THEFT IN THE CYBER SCOPE FROM THE PERSPECTIVE OF NATIONAL CRIMINAL LAW

**Deny Prabowo [1*] Muhammad Arif Sahlepi [2*]**
[12] Universitas Pembangunan Panca Budi
*E-mail: bungbw@gmail.com arifsahlepi@dosen.pancabudi.ac.id*

**Article Info**
**Article History**
Received: 2025-05-05
Revised: 2025-05-06
Published: 2025-06-06

**Keywords:**
*Digital Identity Theft, Victim Protection, Criminal Law Reform.*

**Abstract**
This study critically and in-depth examines the form and effectiveness of legal protection for victims of cyber identity theft within Indonesia's national criminal law system. Although Indonesia has legal instruments such as the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Personal Data Protection Law (UU PDP), in reality, victim protection remains very weak, formalistic, and non-operational. Victims of digital crime are left to struggle alone in a legal system that is slow, procedural, and lacks empathy. The offender-centered legal approach marginalizes victims' rights, even though identity theft directly impacts the honor, reputation, and security of citizens. This study uses a normative juridical method with a conceptual approach, analyzing various laws and regulations, victimology theory, legal protection doctrine, and jurisprudence. The results show that in addition to the lack of regulation in the Criminal Code regarding data as an object of crime, there is still fragmentation between institutions, weak digital forensic support, and the absence of an appropriate and victim-friendly recovery mechanism. The state cannot simply provide norms; it must also establish a concrete, swift, and responsive system to ensure that victims of digital crime receive substantive justice. This research confirms that victim protection must be a key agenda for future Indonesian criminal law reform, not merely legalistic discourse ungrounded in reality.

## I. INTRODUCTION

Advances in information and communication technology in the last two decades have brought humans into a new era known as the digital era.(BAKARA 2024)Digitalization has brought significant benefits in terms of efficiency in communications, economic transactions, education, and public services. However, along with these benefits, serious threats have emerged in the form of cybercrime.(Gift 2024)One form of crime that is growing rapidly is the crime of digital identity theft, namely the act of obtaining, using, or misusing someone's personal data illegally for personal gain or to harm another party.(Annas and Fatiha 2025)

A person's digital identity, including name, National Identification Number (NIK), address, telephone number, biometric information, social media accounts, and financial data, has strategic value and can be used by perpetrators to commit various further crimes. The losses suffered by victims vary, ranging from financial loss and reputational damage to psychological distress and legal challenges due to the use of personal data in unlawful acts.(Safalla 2024)

According to data from the Global Business Guide (GBG) Indonesia in 2023, losses due to digital identity theft in Indonesia have exceeded Rp 500 billion, with the number of cases increasing by 25% compared to the previous year.(Kholiviya 2021)Meanwhile, a report from the Cyber Crime Directorate of the Indonesian National Police's Criminal Investigation Agency (Bareskrim Polri) shows that identity theft often occurs through the misuse of personal data for online loan fraud, bank account hacking, digital document forgery, and the creation of fake accounts.(Ponglabba 2024)

One case that has garnered public attention is that of Renaldy Bosito. He was the victim of identity theft, where his personal data was used by an unknown party to access digital financial services and apply for online loans in his name. As a result, he faced claims for fictitious debts. Despite reporting the case to the authorities, the

legal process was slow, and restitution was not immediately possible. This case illustrates that legal protection for victims of identity theft still faces various structural and normative obstacles.

From a legal perspective, Indonesia already has several laws and regulations that can be used to prosecute perpetrators of identity theft. The Criminal Code (KUHP) is a general criminal code that has long been used as the basis for prosecuting various crimes, including theft, fraud, and forgery. However, the new Criminal Code, enacted through Law Number 1 of 2023, still maintains the definition of theft in the form of tangible objects, thus not explicitly addressing digital data as an object of theft. Nevertheless, the articles related to fraud and forgery in the new Criminal Code can still be used in the context of digital identity theft.

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), along with its amendments through Law Number 19 of 2016 and Law Number 1 of 2024, provides a specific legal basis for crimes in the digital space. Article 30 in conjunction with Article 46 prohibits illegal access to electronic systems, and Article 32 in conjunction with Article 48 regulates the illegal acquisition and transmission of data. Meanwhile, Article 35 in conjunction with Article 51 regulates electronic data falsification. These provisions serve as an important foundation for prosecuting perpetrators of identity theft in the digital space.(Zuraini 2025)

Furthermore, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) strictly prohibits the unauthorized acquisition, use, and disclosure of personal data. Article 67 of the PDP Law carries a maximum prison sentence of five years and/or a fine of up to five billion rupiah for anyone who illegally obtains or collects another person's personal data. Articles 68 and 69 of the PDP Law also stipulate criminal penalties for those who disclose or use personal data without authorization, as well as for those who falsify personal data.

Despite progress in regulatory aspects, the effectiveness of legal protection for victims is still suboptimal. Many victims are unaware of the legal procedures for obtaining redress, such as restitution, reputation rehabilitation, or deletion of misused data. Furthermore, the law enforcement process still faces various challenges, ranging from limited investigator capacity in digital forensics, a lack of human resources in the cyber field, to a lack of synchronization of mechanisms between institutions such as the Police, the Ministry of Communication and Information, the Financial Services Authority (OJK), and the Witness and Victim Protection Agency (LPSK).(Kholiviya 2021)

Victimology theory emphasizes the importance of legal support for victims of crime. Victims should not only be positioned as tools to prove the perpetrator's guilt, but also as legal subjects with the right to restitution. Satjipto Rahardjo's thinking on progressive law emphasizes that the law must side with the weak and vulnerable. In this context, victims of identity theft are in a structurally and socially weak position, necessitating substantive legal support.

On the other hand, the constitutional mandate in Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that: "Everyone has the right to recognition, guarantees, protection and certainty of fair law and equal treatment before the law." This norm emphasizes the state's obligation to provide legal protection to every citizen, including against digital crimes such as identity theft.

Over time, several concrete cases have highlighted gaps in the national legal system in addressing identity theft. The "Handsome" syndicate in Bogor (2024) used an illegal app to steal the National Identity Number (NIK) data of thousands of citizens; the OTP syndicate in Denpasar (2024) misused personal data for fictitious transactions; and the identity theft case involving a Malaysian citizen using fake BTS techniques in Jakarta (2025) demonstrate that identity theft has become a complex transnational crime. Although some perpetrators have been successfully prosecuted under the ITE Law and the Personal Data Protection Law, victim recovery remains a key focus.(Puspitosari and Kusumaningrum 2021)

Considering the escalating prevalence of identity-based cybercrime and the challenges facing the legal system in ensuring victim protection and recovery, this research is crucial. It aims to evaluate existing legal regulations, analyze the forms of legal protection available to victims, and identify obstacles and needs for criminal law reform that are more responsive to identity theft-based cybercrime.

Based on the description above, the problem formulation in this research is:

1. What are the legal provisions regarding the crime of identity theft in cyberspace according to the latest Criminal Code and

applicable laws and regulations in Indonesia?
2. What form of legal protection is provided to victims of cyber identity theft crimes in the national criminal law system, and what are the obstacles to its implementation?

## II. RESEARCH METHODS

The research method used in this study is a normative juridical method with a conceptual approach.(Indra Utama Tanjung 2024)A normative juridical approach is used to examine and analyze positive legal norms governing the protection of victims of identity theft in cyberspace. The analysis focuses on applicable laws and regulations, such as the latest Criminal Code (KUHP) in Law Number 1 of 2023, Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 in conjunction with Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). A conceptual approach is used to support the study of relevant legal theories, particularly the theory of legal protection, the theory of victimology, and the principle of justice in criminal law. The data used in this study are entirely secondary data, classified into three types: primary legal materials in the form of laws and regulations, minutes of lawmaking, and court decisions; Secondary legal materials include legal literature, scientific journals, legal articles, research results, and related theses or dissertations; and tertiary legal materials include legal dictionaries, legal encyclopedias, and legislative directories.(Fikran 2025)

The data collection technique was conducted through library research by searching for legal documents in both printed and digital forms through official sources such as the websites of the Supreme Court of the Republic of Indonesia, the Witness and Victim Protection Agency (LPSK), the Ministry of Communication and Information, the National Legal Aid Agency (BPHN), and scientific journal portals such as Google Scholar, Garuda, and Sinta. All collected data were analyzed in a juridical-qualitative manner, namely by classifying legal issues based on problem formulation, normative interpretation of relevant statutory provisions, and constructing legal arguments based on theory and doctrine.(Hutabarat 2024)This analysis was conducted not only to describe the applicable regulations (descriptive), but also to evaluate the effectiveness of existing legal norms and develop critical recommendations for improving the protection system for victims of digital identity crime. Thus, this method provides a strong foundation for research that is not only theoretical, but also solution-oriented and reflective of the challenges of legal implementation in the digital age.

## III. RESULTS AND DISCUSSION

### A. Legal Regulations Regarding the Crime of Identity Theft in Cyberspace According to the Laws and Regulations in Force in Indonesia

The rapid development of information technology has given rise to new forms of crime that not only cause financial losses but also threaten human rights, including the right to privacy and personal data protection. One increasingly disturbing form of crime is digital identity theft, the unlawful act of taking, using, or falsifying someone's digital identity for profit or to harm the victim.(Gultom 2024)In this context, Indonesian national criminal law has provided a number of normative bases for prosecuting perpetrators and providing protection for victims. These provisions are spread across various legal instruments, including general criminal law (the Indonesian Criminal Code), specific criminal laws (the Electronic Information and Transactions Law and the Privacy Law), and supporting laws such as witness and victim protection (Law 13/2006 in conjunction with Law 31/2014) and other implementing regulations.

#### 1) Criminal Code (KUHP)

The Indonesian Criminal Code (KUHP) is the primary source of substantive criminal law in Indonesia. Although the KUHP does not explicitly recognize the term "digital identity theft," several general provisions can still be used to prosecute perpetrators.(Diansah, Usman, and Monita 2022)One of the most relevant articles is Article 378 of the Criminal Code concerning fraud. This article reads:

*"Anyone who, with the intention of unlawfully benefiting himself or another person, by using a false name or false dignity, by deception, or by a series of lies, induces another person to hand over something to him, or to grant a loan or to write off a debt, is threatened with fraud, with a maximum imprisonment of four years."*

This provision can be used to prosecute perpetrators who use false identities to commit online fraud, such as opening online loan accounts in someone else's name. The element of using a "fake name" in this article is highly relevant to addressing forms of digital impersonation that occur on various internet platforms.(Gulo 2023)

In addition to Article 378, Articles 263 and 264 of the Criminal Code concerning document forgery can also be used to prosecute identity theft perpetrators who falsify identity documents such as KTPs, SIMs, or digital population documents. Article 263 states that:

*"Anyone who makes a false letter or falsifies a letter that can give rise to a right, obligation or release from debt, or which is intended as evidence of something with the intention of using or ordering another person to use the letter as if its contents were true and not false, is threatened with a maximum prison sentence of six years."*

If the forged documents are used to open a bank account, create an online account, or apply for a loan illegally, the perpetrator's actions can be considered document forgery under the law. Furthermore, Article 266 of the Criminal Code imposes criminal penalties on anyone who knowingly uses forged documents in legal or administrative proceedings as if they were legitimate and genuine.(Popal 2023)

However, because the Criminal Code was drafted long before the digital era, its provisions fail to capture the complexity of cybercrimes, which target personal data and digital identities rather than tangible objects. To address this gap, a specific regulation governing criminal acts in the digital space is needed, namely the Electronic Information and Transactions Law (UU ITE).

**2) Electronic Information and Transactions Law (ITE Law)**

Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 in conjunction with Law No. 1 of 2024 concerning Electronic Information and Transactions is a special regulation designed to address legal challenges in the digital era.(Prakoso, Sujana, and Suryani 2020)The ITE Law regulates various forms of legal violations in cyberspace, including illegal access, electronic data manipulation, and digital identity forgery.

One of the important articles is Article 30 of the ITE Law which reads:

*"Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way."*

This illegal access is the starting point for many cases of digital identity theft. Perpetrators who hack into someone's system or online account with the intention of stealing their personal data are violating this provision. Article 46 of the ITE Law stipulates criminal penalties for such violations, with imprisonment of up to six years and/or a fine of up to IDR 600 million.

Furthermore, Article 32 of the ITE Law prohibits changing, adding, reducing, transmitting, damaging, removing, moving, or concealing another person's electronic information. This provision covers data theft, whether with the intent to store, sell, or misuse it. In practice, identity theft often involves copying personal data from electronic systems such as e-commerce servers, banking systems, or social media platforms.(Bahri 2023)

Digital identity forgery is specifically regulated in Article 35 of the ITE Law, which states:

*"Any person who intentionally and without authority or against the law manipulates, creates, changes, removes, or destroys Electronic Information and/or Electronic Documents with the aim of making the Electronic Information and/or Electronic Documents appear to be authentic data."*

This forgery can include creating fake accounts with the victim's name and photo, using doctored digital documents, or filling out online forms using another person's personal data. These acts are punishable by a maximum prison sentence of 12 years and/or a maximum fine of IDR 12 billion, as stipulated in Article 51 paragraph (1) of the ITE Law.(2022 Award and Tantimin)

It is important to note that the recent amendment to the ITE Law through Law No. 1 of 2024 has introduced an official definition of "digital identity," which is defined as "Electronic Information containing the unique identity of a legal entity whose use is under the control of that legal entity." This recognition clarifies that unauthorized use of digital identity can be categorized as a criminal offense.

**3) Personal Data Protection Act (PDP Act)**

The most significant regulation addressing digital identity theft in Indonesia is Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law was enacted in response to increasing personal data breaches, including the illegal trading of citizen identity data online, particularly on the black market.(Dzaki 2025)

Article 65 of the Personal Data Protection Law explicitly prohibits any person from

unlawfully obtaining or collecting personal data that does not belong to them, for the purpose of benefiting themselves or another party, if such action could cause harm to the Personal Data Subject. The types of data protected include identity data (such as National Identity Numbers (NIK) and National ID Cards (KTP), addresses, and biometric data, including facial and fingerprint data.

Article 65 of the PDP Law explicitly states:

*Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to the Personal Data Subject.*

Furthermore, Article 66 prohibits anyone from falsifying personal data with the intention of harming the data subject or gaining a specific advantage. This includes creating fake accounts using another person's identity, falsifying official documents, and manipulating consumer data for fraud.

The criminal sanctions imposed for this violation are quite severe, as regulated in:

- Article 67: Violations of the provisions of Article 65 are subject to a maximum prison sentence of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah).
- Article 68: Violations of Article 66 are punishable by imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 6,000,000,000 (six billion rupiah).

It is important to note that these sanctions do not only target the main perpetrators of data theft or misuse, but can also be imposed on parties who illegally obtain, purchase, or utilize personal data, including corporations or third parties who receive data without the data subject's consent.(Mewengkang 2021)

With the enactment of the Personal Data Protection Law, the Indonesian legal system now has a specific legal basis that affirms personal data as a constitutionally protected right, not merely technical information. This law shifts the approach from solely punishing perpetrators to comprehensive protection of individuals' rights to their personal data, while also promoting accountability for all parties managing data.

**4) Witness and Victim Protection Law (Law 13/2006 jo. Law 31/2014)**

In the context of identity theft victims, it is also important to consider the legal protection aspects for the individuals who have been harmed. Law No. 13 of 2006 concerning Witness and Victim Protection, as amended by Law No. 31 of 2014, provides several important rights to victims of crime, including victims of digital crime.(Rofiqoh, nd)

Article 5 states that victims have the right to:

*"Receive protection for the security of oneself, family, and property from threats related to testimony that will be, is being, or has been given; receive information regarding case developments; and receive legal assistance."*

Furthermore, Article 5 paragraph (1) letter i specifically states that victims have the right to "obtain a new identity and/or obtain a new residence" if their existence is threatened. This provision is important in serious cases of identity theft where the victim receives threats from the perpetrator or experiences secondary victimization due to the dissemination of personal data.(Flora et al. 2024)

This law also paves the way for victims to seek restitution or compensation from perpetrators as a form of reparation for material and psychological losses. The Witness and Victim Protection Agency (LPSK) can facilitate this process and provide assistance throughout the legal process.

**5) Implementing and Supporting Regulations**

In addition to laws, there are also implementing regulations that strengthen efforts to combat digital identity theft. For example, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), which requires electronic system operators to maintain the confidentiality, integrity, and security of user personal data. This regulation serves as a technical reference for agencies or companies that manage user data to implement adequate cybersecurity systems.(Gift 2024)

Similarly, Minister of Communication and Information Technology Regulation No. 20 of 2016 regulates the principles of personal data protection in electronic systems, such as the requirement to obtain data owner consent, the obligation to store data securely, and restrictions on data processing. While it does not contain direct criminal sanctions, this regulation provides an ethical and administrative basis that can be used to assess the negligence or deliberate negligence of system administrators in safeguarding user data.

Based on the above description, it can be concluded that Indonesian national criminal law

provides adequate regulatory tools to regulate and address digital identity theft. The Criminal Code (KUHP) provides a general basis for criminalizing fraud and identity forgery. The ITE Law expands the scope of offenses to the electronic realm, including unauthorized access and falsification of electronic data. The PDP Law provides specific protection for personal data as a protected legal object, while the Witness and Victim Protection Law guarantees victims' rights to security, recovery, and restitution.(Zamayya et al. 2025)

However, implementation challenges remain significant. Weak law enforcement, a lack of digital forensic investigator capacity, and low public awareness of personal data protection pose serious obstacles to handling digital identity theft cases. Therefore, strengthening systems, increasing the capacity of law enforcement, and conducting public awareness campaigns are strategic steps that must be implemented in parallel with strengthening existing regulations.

## B. Forms of Legal Protection Provided to Victims of Cyber Identity Theft in the Indonesian Criminal Law System, and What Are the Obstacles to Its Implementation?

Victim protection is a crucial principle in the modern criminal justice system, particularly in addressing rapidly growing cybercrimes such as digital identity theft. In Indonesia, the shift in criminal law from a retributive to a corrective and restorative approach has begun to shift attention not only to the perpetrators but also to the restoration of victims' rights. In this context, the protection of victims of digital identity theft becomes relevant to examine, given its direct impact on citizens' rights to privacy, reputation, and even financial security.(Purnama and Haris 2024)

Digital identity theft is generally committed by unauthorized access, acquisition, and use of a person's personal data for harmful purposes. This crime can be committed through hacking digital accounts, phishing, misuse of online registration systems, and even falsification of electronic documents. The consequences for victims can be complex: from financial loss due to misuse of data in financial transactions, to defamation, to psychological distress due to identity data being used for crimes they did not commit. Therefore, the Indonesian criminal justice system is required to provide legal protection that is not only repressive for perpetrators, but also curative and rehabilitative for victims.

### 1) Protection from a Material Criminal Law Perspective

In the Indonesian criminal law system, protection for victims of digital identity theft is found in at least three groups of regulations: general criminal law (KUHP), special criminal law (ITE Law and PDP Law), and victim protection law (Witness and Victim Protection Law).(Tuju, Ramadani, and Nasution 2025)

*First*The Criminal Code (KUHP) contains several provisions that can indirectly be used to prosecute perpetrators of identity theft. Article 378 of the KUHP regulates fraud, which involves the use of a "false name" or "false dignity" to deceive others and obtain unlawful benefits. In the context of cybercrime, this element is relevant when the perpetrator illegally uses another person's identity to gain access to financial facilities or other rights in the victim's name.

Additionally, Articles 263 and 264 of the Criminal Code concerning document forgery can be invoked if the perpetrator falsifies identity documents, such as a digital ID card or a digital copy of a population certificate. Although the Criminal Code does not explicitly recognize personal data as an object of crime, in practice, the formulation of the Criminal Code offense is still used as the basis for law enforcement in cases that do not yet have lex specialis provisions.

*Second*The introduction of the Electronic Information and Transactions Law (UU ITE) broadens the criminal law regime by including acts in the electronic space as a crime. Article 30 of the ITE Law explicitly prohibits unauthorized access to another person's electronic systems. Criminal sanctions stipulated in Article 46 of the ITE Law can reach up to six years in prison. Perpetrators who access email accounts, social media accounts, or online service provider databases without permission with the intention of obtaining user identity information can be prosecuted under this provision.

Article 32 of the ITE Law expands the offense to include altering, removing, or concealing another person's electronic information. This is relevant in cases where the perpetrator steals or deletes a person's identity data from an electronic system, either for personal use or for sale to a third party. The criminal penalty imposed can be up to eight years in prison, as stipulated in Article 48 of the ITE Law.(Rizkiyanto, Sudewo, and Rizkianto 2024)

More specifically, Article 35 of the ITE Law regulates the falsification of electronic information, namely acts committed with the

intention of making electronic documents appear authentic. In practice, this offense is used against perpetrators who create fake accounts or fake digital-based documents in the name of the victim. Perpetrators can be subject to a maximum prison sentence of twelve years and/or a fine of IDR 12 billion as stipulated in Article 51 paragraph (1) of the ITE Law. Thus, the ITE Law provides direct criminal protection to victims by providing a basis for criminalization for perpetrators of data theft and digital identity falsification.

*Third*Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is the latest law that explicitly recognizes personal data as a legal entity that has legal protection. Article 65 of the PDP Law states that everyone is prohibited from obtaining or collecting personal data belonging to others unlawfully. The criminal threat for this violation is up to five years in prison and/or a maximum fine of IDR 5 billion as stipulated in Article 67 paragraph (1) of the PDP Law. Identity theft perpetrators who illegally misuse data such as NIK, name, address, and victim biometrics can clearly be prosecuted under this provision.

Furthermore, Article 66 of the PDP Law prohibits the creation or falsification of personal data for personal gain or to the detriment of others. This provision accommodates criminal scenarios where the perpetrator not only steals data but also uses it for other criminal acts. The criminal penalty is up to six years in prison and/or a maximum fine of IDR 6 billion (Article 68 of the PDP Law). From a substantive criminal law perspective, the PDP Law progressively positions personal data as a protected legal object, and makes violators of data subjects' rights criminals.

**2) Protection from the Perspective of Formal Criminal Law and Procedural Law**

From a criminal procedural law perspective, victim protection is accommodated in Law No. 13 of 2006 in conjunction with Law No. 31 of 2014 concerning Witness and Victim Protection (PSK Law). Although it does not specifically mention victims of digital identity theft, this law provides all victims of crime with the right to legal protection, legal aid, psychological support, and rights restoration.

Article 5 of the Sex Workers Law states that victims have the right to a sense of security, legal assistance, information regarding the legal process, and assistance with compensation and restitution. Specifically in the context of identity theft, the provisions of Article 5 paragraph (1) letter i allow victims to apply for a change of identity or residence if there is a threat to their safety. This provision is important to provide a sense of security for victims whose identities have been used for criminal activities, especially if the victim experiences threats, intimidation, or other forms of digital revictimization.(Fadilah, Aranggraeni, and Putri 2021)

The Witness and Victim Protection Agency (LPSK) has the authority to provide physical protection, psychological assistance, medical assistance, and legal advocacy to victims. Furthermore, the LPSK can also facilitate restitution claims against perpetrators, as stipulated in Article 7A of the Law on Sexual Assault. Restitution can include compensation for material losses, medical expenses, and even restoration of reputation.(Gemilang, Ismaidar, and Zarzani 2024)In some serious cases, compensation can be provided by the state if the perpetrator is unable to fulfill the restitution obligation.

From this procedural legal framework, it appears that the legal system provides victims with access to substantive justice through mechanisms for redress and protection against potential threats. However, the effectiveness of these mechanisms is not without implementation challenges, both at the regulatory, institutional, and social levels.

**3) Civil and Administrative Protection**

Victim protection can also be achieved through civil and administrative channels. In civil law, Article 1365 of the Civil Code provides a basis for victims to file a lawsuit for unlawful acts against perpetrators who have used their personal data without authorization. Perpetrators can be sued for unlawful acts if it can be proven that the actions have caused harm.

The PDP Law also regulates the civil rights of victims as data subjects, including the right to information, the right to access, the right to rectification, the right to erasure, and the right to object to data processing. Article 8 of the PDP Law states that data subjects have the right to withdraw consent to the processing of their personal data. If the data controller does not comply with this request, victims can file a complaint with the personal data protection authority.(Sabadina 2021)

In practice, the Ministry of Communication and Information Technology (Kominfo) uses a public complaints mechanism to open channels for removing content and processing personal data that violates user rights. Prior to the PDP Law's effective date, Ministerial Regulation No. 20 of 2016 served as a reference in this regard. This

provides administrative means for correcting and restoring victim data through official government-regulated channels.

**4) Implementation Obstacles in Victim Protection**

Despite the existence of a normative legal framework, the implementation of legal protection for victims of digital identity theft still faces significant challenges. Implementation challenges face at least four aspects: substantive law, institutional, technical, and socio-psychological.

*First*From a substantive legal perspective, Indonesia currently lacks a specific criminal offense using the nomenclature "digital identity theft" in its Criminal Code or other sectoral laws. This has led law enforcement officials to rely on general articles that do not always reflect the complex nature of digital crimes. Consequently, investigators often struggle to charge perpetrators with appropriate charges, or courts are unable to award restitution due to the lack of explicit provisions in the Criminal Code.

*Second*From an institutional perspective, the implementation of protection through the LPSK (Lembaga Masyarakat Pemberantasan Korupsi) and law enforcement agencies remains hampered by a lack of human resources competent in cybercrime. The LPSK Chairperson acknowledged that although the law allows victims to change their identities, administratively, this remains difficult, requiring cross-sector coordination with the Directorate General of Civil Registration, the police, and the courts. The identity change procedure is often lengthy and unfriendly to victims seeking to quickly recover from the impact of crime.

*Third*Technically, proving digital identity theft requires advanced digital forensic skills and data tracing technology. In many cases, perpetrators disguise their tracks through VPNs, fake accounts, or overseas servers. This complicates identification and slows down investigations. Meanwhile, speed is crucial in combating cybercrime, as the longer data is released, the greater the losses to victims.(Silalahi, Sahlepi, and Sidi 2024)

*Fourth*From a social and psychological perspective, many victims are reluctant to report the crime for fear of being blamed or re-victimized. Some victims are unaware that their identity has been stolen and only realize it after receiving a bill or being summoned by law enforcement for an act they did not commit. Studies show that victims of identity theft often experience psychological distress and a loss of trust in the legal system that fails to promptly respond to their complaints.

On the other hand, low digital literacy also contributes to high levels of vulnerability. Many individuals voluntarily share their personal data without realizing the risks involved. Ignorance of their legal rights prevents them from reporting identity theft or pursuing their rights, such as restitution, restoration of reputation, or data deletion.(Fazizullah, Marlina, and Sahlepi 2022)

In addition to the factors mentioned above, there are also obstacles to harmonizing the substance of new regulations, such as the latest Criminal Code (KUHP), with relevant sectoral laws. The new Criminal Code, through Law Number 1 of 2023, still maintains the classic approach to the offenses of theft, fraud, and forgery involving tangible objects, thus not explicitly designating personal data as an object of crime. In practice, law enforcement officers must rely on legal constructions that adapt these articles to make them relevant to cyberspace. This inevitably creates interpretive gaps that can lead to a weakening of victims' positions in court. The lack of explicit recognition in the Criminal Code of identity theft as a specific offense leads authorities to rely more heavily on the ITE Law and the PDP Law, which unfortunately have not been fully integrated with national criminal procedure law.(Saragih and Sahlepi 2019)

On the other hand, although Law Number 27 of 2022 concerning Personal Data Protection provides more progressive norms in recognizing the rights of data subjects, including the right to compensation and data deletion, its implementation remains hampered by institutional issues and the lack of an effective data oversight authority. The personal data protection authority, as mandated by the Personal Data Protection Law, is still in the structural and operational stages of formation. As a result, many victims lack clear administrative channels to file complaints or seek redress. When the rights promised in legal norms are not followed up with concrete mechanisms accessible to the public, the state's presence in protecting victims is merely symbolic, not substantive.(Sihombing, Sahlepi, and SH, nd)

Furthermore, the absence of implementing regulations (government regulations or ministerial regulations) that technically regulate identity recovery procedures, civil lawsuit mechanisms for data misuse, or standardization of personal data security by public and private

institutions, worsens the legal situation of victims.(Meliala and Sahlepi 2024)Without procedural clarity and technical substance, law enforcement officials will be confused in following up on victims' reports, while victims themselves will lose hope of justice. This situation demonstrates the need for not only normative reforms in national criminal law but also the need to mainstream victim protection throughout Indonesia's legal system, particularly for information technology-based crimes such as digital identity theft.

**5) Reflection and Urgency of Strengthening Protection**

Given the above conditions, legal protection for victims of digital identity theft in Indonesia remains partial and reactive. This crime, however, has unique characteristics: it crosses jurisdictional boundaries, spreads rapidly, and causes significant psychosocial harm.(Fazizullah, Marlina, and Sahlepi 2022)Therefore, there needs to be a holistic approach that integrates normative legal protection, victim recovery policies, and responsive support systems.

Strengthening needs to be done in several aspects: first, encouraging the codification of specific offenses in the Criminal Code or the creation of a separate law regarding identity crimes; second, increasing the capacity of the LPSK, Kominfo, and other law enforcement agencies in handling victims of digital crimes; third, accelerating the harmonization of the population administration system with victim protection so that identity changes can be carried out effectively; and fourth, expanding digital legal literacy programs to the public to be more vigilant and proactive in protecting their personal data.

Thus, in the future, the national criminal law system is expected to not only be able to punish perpetrators of identity crimes, but also restore the rights and dignity of victims in full, in the spirit of restorative justice and human rights protection.

## IV. CONCLUSIONS AND RECOMMENDATIONS

Legal protection for victims of digital identity theft in Indonesia remains little more than a normative slogan without any concrete structural implementation. The state appears slow, even negligent, in establishing a legal mechanism that fully supports victims whose digital rights and legal dignity have been violated. Although the new Criminal Code, the Electronic Information and Transactions Law, and the Privacy and Personal Data Law have provided a legal foundation, their implementation has been hampered by overlapping norms, weak enforcement, and a lack of literacy among officials and the public. Victims are left to fend for themselves in a maze of bureaucracy and uncertainty, without certainty of identity restoration, compensation, or a sense of security. In a nation based on the rule of law that claims to uphold justice, this situation is a stark irony that reflects a structural failure to position victims at the center of the criminal justice process. It is time for victim protection to cease being an appendix to the prosecution of perpetrators, but instead become a core mandate of a vibrant, progressive, and responsive legal system to digital challenges.

## REFERENCE LISTAN

Annas, Gilang Kresnanda, and Nilam Fatiha. 2025. "LEGAL PROTECTION FOR VICTIMS OF CYBER CRIME: CHALLENGES AND SOLUTIONS." JOURNAL OF KLIENDI LAW 2 (1): 98–114.

Anugerah, Fiqqih, and Tantimin Tantimin. 2022. "Personal Data Theft on the Internet from a Criminological Perspective." Journal of Legal Communication (JKH) 8 (1): 419–35.

Bahri, Idik Saeful. 2023. Cyber Crime in the Spotlight of Criminal Law (2023 Edition). Bahasa Rakyat.

BAKARA, PAUL LUNDU. 2024. "LEGAL PROTECTION FOR VICTIMS OF DIGITAL IDENTITY THEFT IN CYBERCRIME."

Diansah, Hendri, Usman Usman, and Yulia Monita. 2022. "Criminal Law Policy on Carding Crimes." PAMPAS: Journal of Criminal Law 3 (1): 15–30.

Dzaki, Arly Habibi. 2025. "VICTIMOLOGY ANALYSIS OF THE OCCURRENCE OF PERSONAL DATA THEFT CRIME THROUGH ELECTRONIC MEDIA (Study at Lampung Regional Police)."

Fadilah, Andi, Renda Aranggraeni, and Sri Reski Putri. 2021. "The Existence of Cyber Security Against Cyberstalking Acts in the Cybercrime Criminal Accountability System." Syntax Literate: Indonesian Scientific Journal 6 (4): 1555.

Fazizullah, Fazizullah, Marlina Marlina, and Muhammad Arif Sahlepi. 2022. "Legal Study of Narcotics Crimes Based on Law Number 35 of 2009 Concerning Narcotics in the Banda Aceh Region (Study of Decision Number: 248/Pid. Sus/2015/PN Bna)." Al-

Hikmah Law Journal: Media for Communication and Information on Law and Society 3 (2): 304–25.

Fikran, Maulana. 2025. "Review of Islamic Criminal Law on Cyber Crime in the Form of Personal Data Theft." Journal of Criminal Law and Legal Politics 10 (2): 1–18.

Flora, Henny Saida, M SH, M Kn, MH Kes, SH Kasmanto Rinaldi, M SI, SH Jusri Mudjrimin, SH Sitta Saraya, SH Yusrina Handayani, and SH Ratna Jaya. 2024. Criminal Law in the Digital Era. CV Rey Media Grafika.

Gemilang, Gilang, Ismaidar Ismaidar, and T Riza Zarzani. 2024. "Corporate Criminal Liability in Money Laundering Crimes." Innovative: Journal Of Social Science Research 4 (2): 8455–71.

Gulo, Karunia Krisman. 2023. "Legal Protection for Victims of Fraud Using Android Package Applications Through WhatsApp Messages (Study at the Special Criminal Investigation Directorate of the North Sumatra Regional Police)."

Gultom, Regina Yustine. 2024. "Legal Considerations of Judges and Legal Protection for Victims of Fraud in Online Buying and Selling Transactions on Facebook Social Media (Study of Batang District Court Decision Number: 6/Pid. Sus/2021/PN. BTG)." Indonesian Christian University.

Hutabarat, Mario Valentino. 2024. "LEGAL PROTECTION FOR PHISHING CRIMINAL VICTIMS ACCORDING TO LAW NUMBER 19 OF 2016 CONCERNING AMENDMENTS TO LAW NUMBER 11 OF 2008 CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS." FACULTY OF LAW, ISLAMIC UNIVERSITY OF NORTH SUMATRA.

Indra Utama Tanjung. 2024. BASICS OF LEGAL RESEARCH METHODS. Karanganyar: CV Pustaka Dikara). https://scholar.google.com/citations?view_op=view_citation&hl=id&user=rToGqjUAAAAJ&cstart=20&pagesize=80&citation_for_view=rToGqjUAAAAJ:Wp0gIr-vW9MC.

Kholiviya, Hasna. 2021. "Legal Protection for Victims of Personal Data Theft in Cyber Crime Cases." Sultan Agung Islamic University, Semarang.

Kurnia, Ichwan. 2024. "Cyber Criminal Law: Theoretical and Practical Aspects in the Digital Era in Indonesia."

Meliala, Nugraha Manuella, and Muhammad Arif Sahlepi. 2024. "Implementation of Restorative Justice by the Medan District Court to Achieve Legal Certainty in Resolving Criminal Acts." Journal of Law, Humanities and Politics 4 (3): 459–70.

Mewengkang, Indriani Berlian. 2021. "Legal Study of Cyber Crime Prevention and Law Enforcement." Lex Crimen 10 (5).

Ponglabba, Gilbert. 2024. "Protection for Victims of Personal Data Theft (Reviewed Based on Law Number 27 of 2022, Concerning Personal Data Protection)." Christian University of Indonesia.

Popal, Daniel F T. 2023. "Efforts to Combat Cyber Crime." Lex Administratum 11 (5).

Prakoso, Bagus Andi Dwi, I Nyoman Sujana, and Luh Putu Suryani. 2020. "Legal Protection for Victims of Online Buying and Selling Fraud." Journal of Legal Construction 1 (2): 266–70.

Purnama, Yan Fathahillah, and Oheo Kaimuddin Haris. 2024. "Cyberstalking as an Unlawful Act in Indonesian Criminal Law." Halu Oleo Legal Research 6 (1): 103–21.

Puspitosari, Hervina, and Anggraeni Endah Kusumaningrum. 2021. "Victim Impact Statement as an Effort to Provide Legal Protection for Female Victims of Revenge Porn." USM Law Review Journal 4 (1): 67–81.

Rizkiyanto, Eka, Fajar Ari Sudewo, and Kus Rizkianto. 2024. Law Enforcement Against Cyberbullying Crimes Through Electronic Media. NEM Publisher.

Rofiqoh, Anita Zulfiani. nd "Unraveling the Phenomenon of Cybercrime in the Realm of Economic Criminal Law: Presenting New Challenges for Law Enforcement in the Digital Era."

Sabadina, Uni. 2021. "Criminal Law Politics for Combating Information Technology Crimes Related to Personal Data Leaks by Online-Based Corporations." Lex Renaissance 6 (4): 799–814.

Safalla, Nansya Janaika. 2024. "LEGAL PROTECTION OF CONSUMERS AGAINST CRIMINAL ACTS OF PERSONAL DATA THEFT IN E-COMMERCE TRANSACTIONS IN INDONESIA." Sultan Agung Islamic University Semarang.

Saragih, Yasmirah Mandasari, and Muhammad Arif Sahlepi. 2019. "Wiretapping Authority in Eradicating Criminal Acts of Corruption." Criminal Law and Legal Development 1 (2).

Sihombing, Frans Answaldo, M Arif Sahlepi, and M SH. nd "Legal Analysis of Criminal Acts of Violence Against Other People Committed Together." Panca Budi Journal 1 (1).

Silalahi, Haposan, Muhammad Arif Sahlepi, and Redyanto Sidi. 2024. "Implementation of Alternative Punishments for Minor Crime Offenders as an Effort to Decongess Correctional Institutions." JIIP-Jurnal Ilmiah Ilmu Pendidikan 7 (5): 4657–65.

Tuju, Marselino Clifer, Suci Ramadani, and Chairuni Nasution. 2025. "Law Enforcement Against Cyber Crimes in Online Fraud Cases from a Criminological Perspective." Innovative: Journal of Social Science Research 5 (2): 1763–76.

Zamayya, Andi Rania Risya, Devito Imanda Wagiyanto, Paolo Gibran Joesoef, Richie Evanno Salim, and Tiffany Thendean. 2025. "A Theoretical Study of the Implications of the United Nations Convention Against Cybercrime on the Regulation of Cyber Crime in Indonesia." IKRA-ITH HUMANIORA: Journal of Social and Humanities 9 (2): 343–54.

Zuraini, Zuraini. 2025. "LEGAL ASPECTS OF CYBER CRIME IN PHISHING (INFORMATION THEFT) IN INDONESIA." Malikusslaeh University.