Indonesian Journal *of* Digital Crime *and* Criminal Justice
Vol. 2 No. 1. January 2026. pp. 107-146
E-ISSN: XXXX-XXXX| P-ISSN: XXXX-XXX
Original Research Article

Digital Identity Theft and Criminal Protection of Personal Data in Indonesia

Dahlia Putri Amanda[1]*, Damar Sinatrio Putra[2], Siti Mahira Ahmad Mubarak[3]

[1] Universitas 17 Agustus 1945 Surabaya, Surabaya, Indonesia
[2] Universitas Muhammadiyah Surabaya, Surabaya, Indonesia
[3] Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia
* Corresponding author: dahliaputri@gmail.com

ABSTRACT

Digital identity theft has emerged as a significant cybercrime threat in Indonesia, driven by increasing reliance on digital platforms and the widespread use of personal data in online transactions. Despite the enactment of the Personal Data Protection Law, enforcement challenges remain in effectively addressing identity-related cyber offences. This article examines the legal framework governing digital identity theft in Indonesia and evaluates the adequacy of criminal law protections for personal data. Using normative legal research and comparative analysis, the study explores how identity theft is regulated under existing cybercrime and data protection legislation. The findings indicate that legal protections are fragmented across multiple statutes, leading to inconsistencies in enforcement and interpretation. Moreover, challenges in attribution, cross-border data flows, and weak enforcement capacity hinder effective prosecution of offenders. The article argues that Indonesia requires a more integrated legal framework that combines criminal sanctions with robust data protection mechanisms. It proposes strengthening inter-agency coordination, enhancing digital forensic capabilities, and aligning national regulations with international data protection standards. The study concludes that effective protection against digital identity theft requires both legal harmonization and institutional strengthening.

KEYWORDS: Identity Theft, Personal Data Protection, Cybercrime, Indonesia, Digital Security, Criminal Law, Data Privacy

Available online at https://journal.criminallawinstitute.org/JDCCJ/article/view/24, since January 15, 2026
Submitted: October 21, 2025 ■ Reviewed: November 7, 2025 ■ Revised: December 9, 2025; January 8, 2026 ■ Accepted: January 10, 2026

INTRODUCTION

The contemporary global landscape is characterized by the rapid growth of digital technology and online services, which has fundamentally restructured socio-economic paradigms. This digital transformation has catalyzed the expansion of e-commerce, digital banking, social media platforms, and e-government infrastructure (Sari and Ramli 2022). Consequently, the operationality of these platforms necessitates the increasing collection, storage, and processing of vast amounts of personal data. In the modern digital economy, personal data has emerged as a highly valuable economic asset, often described as the "oil" of the twenty-first century (Zalnieriute 2021). However, the commodification of personal information has concurrently heightened its vulnerability to malicious exploitation, leading to rising incidents of cybercrime targeting personal information globally and domestically.

Among these illicit activities, digital identity theft has surfaced as one of the fastest-growing forms of cybercrime (Bany Mohammed et al. 2023). Digital identity theft involves the unauthorized acquisition, transfer, and fraudulent use of another individual's personal identifying information. The consequences of identity theft are multifaceted and severe, ranging from profound financial losses and fraudulent commercial transactions to systemic reputational harm and unauthorized access to critical digital accounts (Levi 2020). In Indonesia, the growing importance of personal data protection has culminated in significant legislative milestones, most notably the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP). Despite this legislative progress, ongoing enforcement challenges persist, as state institutions struggle to keep pace with the sophisticated methods employed by cybercriminals (Pramono and Utama 2024).

Despite the statutory introduction of the UU PDP, the criminalization and prosecution of digital identity theft in Indonesia remain highly problematic. Identity theft often involves multiple forms of cybercrime—such as phishing, ransomware, and social engineering—and frequently features cross-border activities that defy traditional territorial jurisdiction (Brenner

2021). Currently, legal protections remain fragmented across various statutes, including the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the newly enacted UU PDP, leading to regulatory overlaps and statutory ambiguities.

Furthermore, courts and law enforcement agencies face severe difficulties in determining criminal liability for identity-related offences, particularly regarding corporate liability and intermediary accountability (Greenleaf 2023). These systemic challenges are further compounded by technical bottlenecks in the attribution of perpetrators, complexities in digital evidence collection, obstacles in executing cross-border investigations, and a distinct lack of institutional enforcement coordination (Sulasno 2025). Therefore, there is an urgent need for a comprehensive criminal law response that is robustly integrated with personal data protection frameworks to effectively deter identity-based cybercrimes in Indonesia.

In light of the aforementioned problems, this study formulates several fundamental research questions to guide the inquiry. First, it addresses how digital identity theft is currently regulated under the Indonesian legal framework. Second, it evaluates the extent to which the existing legal framework provides effective criminal protection for personal data. Third, it examines the precise statutory and institutional challenges that arise in prosecuting digital identity theft cases in Indonesia. Finally, it explores the specific legal and policy reforms that are necessary to strengthen the criminal protection of personal data within the national legal system.

In alignment with the research questions, this study establishes clear and targeted objectives. The primary objective is to analyze the systemic legal framework governing digital identity theft in Indonesia. Furthermore, this research aims to evaluate the efficacy of current criminal law protections in safeguarding personal data from digital exploitation. It also seeks to identify and categorize the legal and institutional challenges encountered in law enforcement practices. Ultimately, this study intends to propose structural legal and policy reforms aimed at enhancing data protection mechanisms and optimizing cybercrime enforcement frameworks.

The significance of this study is embedded in both theoretical and

practical dimensions. Theoretically, this study offers a distinct contribution to cybercrime and data protection scholarship, particularly within the context of developing legal systems in Southeast Asia. By examining the intersection of criminal law and data privacy, it advances the theoretical development of legal discourse on digital identity, informational self-determination, and the evolution of privacy rights in the digital era (Floridi 2020). Practically, this research serves as a strategic guidance document for policymakers, law enforcement agencies, regulators, and judicial institutions. The findings provide concrete recommendations for strengthening cybercrime prevention, optimizing digital evidence management, and enhancing judicial adjudication of data-related crimes.

The concept of digital identity encompasses the unique collection of data attributes that represent a physical individual in cyberspace (Windley 2005). Scholar classification delineates categories of personal data into general data, such as full names, gender, and nationality, and specific or sensitive data, which includes biometrics, health data, financial records, and genetic profiles, both of which require differing levels of security architecture (Bygrave 2020). Within digital identity ecosystems, data subjects, data controllers, and data processors interact in complex networks, where the vulnerability of data transmission points increases the risk of exfiltration.

In academic literature, the forms and methods of identity theft are categorized into technical methods, such as hacking, skimming, and credential stuffing, and non-technical methods, which predominantly include social engineering, phishing, and shoulder surfing (Koops et al. 2013). The criminal exploitation of personal information typically serves as a gateway crime, facilitating secondary offences such as online financial fraud, money laundering, and unauthorized digital credit acquisitions (Levi 2020).

This study anchors itself on Alan Westin's informational privacy theory, which posits that individuals must possess the right to control how information about them is communicated to others (Westin 1967). This theory aligns with internationally recognized data protection principles, such as those embedded in the European Union’s General Data Protection Regulation (GDPR), which emphasize lawfulness, purpose limitation, and data

minimization (Hoofnagle, van der Sloot, and Borgesius 2019). From a human rights perspective, data protection is no longer viewed merely as a consumer right, but as an inalienable fundamental human right tied directly to human dignity.

Extensive previous studies have scrutinized identity theft regulation and data breaches globally (Greenleaf 2023; Zalnieriute 2021). Comparative data protection frameworks frequently contrast the stringent, rights-based European model with the sector-specific, market-driven American model (Solove 2024). However, distinct research gaps remain concerning Indonesia; specifically, how the punitive mechanisms of the traditional Indonesian Criminal Code harmonize with the administrative and criminal provisions of the new UU PDP. Most existing Indonesian studies focus solely on the civil liabilities of data breaches, leaving an analytical vacuum regarding comprehensive criminal attribution and cross-border enforcement hurdles.

This study conducts normative legal research, which is a doctrinal method focusing on the analysis of internal coherence, systematic structures, and the vertical and horizontal synchronization of legal norms within the established legal system (Marzuki 2021). To provide a comprehensive and multi-dimensional analysis, this study adopts three distinct methodological approaches. The statutory approach involves examining all relevant Indonesian statutes and implementing regulations addressing cybercrime and data privacy. The comparative law approach compares Indonesia's legal framework with international benchmarks, such as the European Union's GDPR and the Budapest Convention on Cybercrime, to identify systemic legislative solutions. Finally, the conceptual approach utilizes legal doctrines, privacy theories, and criminal liability concepts to address complex issues where statutory law remains silent or ambiguous.

The legal materials utilized in this research are categorized into primary and secondary sources. The primary legal materials consist of binding legal instruments, including Law No. 27 of 2022 on Personal Data Protection, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, the Indonesian Criminal Code, and relevant implementing regulations. The secondary legal materials consist of non-

binding academic sources that provide interpretation and commentary, including high-impact peer-reviewed academic journals, authoritative government reports, cybersecurity briefs from institutions like the National Cyber and Crypto Agency, international legal instruments, and specialized legal textbooks.

The collected legal materials are analyzed through qualitative doctrinal analysis combined with a comparative legal assessment. This process involves the systemic interpretation of texts through grammatical, historical, and teleological methods to derive coherent conclusions regarding criminal liability. Through this descriptive-analytic framework, the study evaluates the gaps between existing legal norms and empirical enforcement realities to formulate structural legislative recommendations.

UNDERSTANDING DIGITAL IDENTITY THEFT

The conceptual framework of digital identity serves as the foundational cornerstone of the modern digital architecture, functioning as the digital representation of physical individuals within cyberspace. Unlike traditional analog identifiers, a digital identity comprises a unique and dynamic compilation of data attributes, ranging from basic demographic parameters to sophisticated cryptographic keys and behavioral biometrics (Windley 2005). Within this ecosystem, digital identity executes critical authentication and identification functions, establishing a baseline of trust necessary to verify that an entity claiming a specific identity is indeed the legitimate owner. Consequently, it plays an indispensable role in digital transactions, acting as the primary conduit for securing financial exchanges, executing e-government services, validating smart contracts, and maintaining the integrity of the broader digital economy.

In contemporary cyber-criminology, identity theft is defined as the unauthorized acquisition, transfer, possession, and illicit use of an individual's personal identifying information without their consent. This offense goes beyond mere data exfiltration, as it culminates in fraudulent impersonation activities where the perpetrator weaponizes the stolen

attributes to deceive third parties, including financial institutions, state agencies, and digital platforms (Koops et al. 2013). By masquerading as the victim, the cybercriminal effectively hijacks the target's legal and economic persona, transforming abstract data points into a functional instrument for illicit gain. This symbiotic relationship between data acquisition and fraudulent deployment emphasizes that identity theft is inherently a process-oriented crime rather than a singular event.

The execution of digital identity theft manifests through several sophisticated methodologies, chief among which are phishing attacks. These credential harvesting schemes utilize advanced social engineering tactics, deceptive hyperlinks, and spoofed interfaces to manipulate unsuspecting users into surrendering their sensitive administrative credentials. Cybercriminals meticulously replicate the aesthetic design of trusted institutions, exploiting human cognitive vulnerabilities such as urgency, fear, or compliance with authority. Once these credentials are systematically harvested, they provide the technical foundation for deep network intrusion, enabling threat actors to bypass multi-factor authentication protocols and establish persistent unauthorized control over targeted systems.

Following the initial acquisition of credentials via phishing or other exfiltration methods, perpetrators routinely engage in extensive account takeover incidents. This phenomenon is characterized by the unauthorized access to and total control of critical digital accounts, ranging from personal electronic mail to centralized digital banking applications (Levi 2020). During an account takeover, the cybercriminal often alters recovery options, changes passwords, and modifies contact information to effectively lock the legitimate user out of their own digital life. This immediate displacement allows the attacker ample time to drain financial balances, extract secondary confidential data, or utilize the hijacked account as a trusted vector to launch subsequent attacks against the victim’s contacts.

Beyond the exploitation of existing accounts, cybercriminals increasingly engage in synthetic identity fraud, which represents a paradigm shift in identity-related cybercrime. This highly sophisticated technique involves the creation of entirely false identities using a strategic blend of real, fabricated,

and compromised personal data, such as combining a legitimate national identification number with a fictitious name and address. Because the fabricated identity does not belong to a single living person, standard fraud detection algorithms often fail to flag the discrepancy, mistaking the synthetic profile for a new consumer building credit. This structural blind spot allows criminal syndicates to maintain these fraudulent identities for years, systematically accumulating credit lines before permanently abandoning them.

This synthetic architecture and its associated fraud vectors are heavily fueled by large-scale data breach exploitation. In this context, vast caches of leaked personal information from corporate or state repositories are weaponized by threat actors, who systematically index, aggregate, and deploy these compromised data sets to perpetrate secondary financial crimes. The proliferation of the dark web has institutionalized this process, turning stolen data into a commodified market asset where illicit actors can buy tailored datasets for targeted attacks (Zalnieriute 2021). The availability of these pre-compiled datasets effectively lowers the technical barrier to entry for identity theft, scaling the volume and velocity of cyber-attacks exponentially.

The ramifications of digital identity theft extend far beyond individual inconvenience, generating catastrophic cascading impacts across multiple layers of society. For the direct victims, the immediate consequences materialize as devastating financial losses and systemic privacy violations, as their personal spheres are compromised and their financial liabilities are artificially inflated through unauthorized credit lines. Victims frequently find themselves suddenly burdened with uncontainable debts, frozen bank accounts, and denial of legitimate financial services due to the fraudulent activities conducted under their names. The process of legally disputing these fraudulent liabilities places a severe psychological and economic strain on the individual, requiring months or even years of administrative remediation.

Furthermore, the enduring reputational damage can severely impair a victim's socio-economic mobility, leading to prolonged legal battles to restore credit ratings and clear wrongfully assigned criminal records (Solove 2024).

When an identity thief commits secondary crimes or financial fraud using a stolen persona, the legal system initially attributes those criminal actions to the innocent data subject. This misattribution can result in wrongful arrests, employment termination, and severe psychological trauma, illustrating how the failure of data protection directly compromises physical safety and liberty. The restoration of a compromised reputation requires substantial evidentiary proof, a burden that often falls unfairly on the victim due to systemic gaps in digital forensics accessibility.

On a macro level, the pervasive proliferation of identity fraud carries severe national cybersecurity implications, as it erodes systemic trust in national digital infrastructures and compromises public sector platforms. When citizens lose confidence in the state's ability to secure its digital identity ecosystem, the adoption rate of essential e-government, digital taxation, and public health platforms plummets significantly. This institutional distrust slows down digital transformation initiatives and forces the state to divert critical fiscal resources away from development and toward defensive cybersecurity mitigation and fraud remediation. Consequently, digital identity theft cannot be viewed merely as an isolated economic crime, but must be treated as a structural threat to state digital sovereignty.

Ultimately, the compounding nature of these threats highlights the absolute necessity of a robust and integrated criminal law framework capable of addressing every stage of the identity theft lifecycle. As digital ecosystems become more interconnected through cloud computing, artificial intelligence, and centralized state databases, the surface area for identity exploitation expands proportionally. The legal apparatus must therefore evolve beyond archaic, siloed definitions of property theft and fraud to encompass the protection of digital personas as an inalienable component of human dignity. Achieving this level of protection requires a synchronized legal strategy that effectively bridges the gap between proactive administrative data governance and retrospective criminal enforcement.

PERSONAL DATA PROTECTION AS A LEGAL INTEREST

The conceptual framing of personal data within the modern digital economy has fundamentally shifted from an abstract privacy concern to a concrete asset of monumental economic value. In the contemporary marketplace, personal information serves as the primary fuel for data-driven business models, where the continuous extraction, aggregation, and algorithmic analysis of consumer behavior generate unprecedented corporate profitability (Zalnieriute 2021). Companies utilize advanced machine learning architectures to transform raw behavioral data into predictive profiles, which are then monetized through targeted advertising, algorithmic credit scoring, and personalized service delivery. Within this context, the traditional boundaries of property and commodity have blurred, establishing personal data as a dual-faceted entity that simultaneously represents an individual's identity and a highly liquid financial asset in global corporate ecosystems. This pervasive commodification, however, creates structural incentives for over-collection, thereby expanding the surface area for security vulnerabilities and illicit data exploitation.

To counteract the risks of systemic commodification, contemporary jurisprudence firmly anchors personal data protection within the doctrine of privacy as a fundamental human right. This rights-based approach possesses distinct constitutional dimensions, as modern democratic states increasingly interpret their founding charters to include the right to informational self-determination, which grants individuals the autonomous power to control the flow of their personal information. Globally, this domestic constitutional evolution is reinforced by international human rights standards, such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, which explicitly shield individuals from arbitrary interference with their privacy (Bygrave 2020). By elevating data protection to the status of an inalienable right, the legal framework establishes that human dignity cannot be bypassed or overridden by market forces or corporate convenience, creating a binding obligation for states to erect robust protective barriers.

The operationalization of this fundamental right is achieved through a set of internationally recognized principles of personal data protection,

beginning with the principle of lawfulness. This foundational standard mandates that any data processing activity must possess a clear, legitimate legal basis under the law, thereby preventing arbitrary or covert data harvesting by either public or private entities. Closely intertwined with lawfulness is the principle of consent, which dictates that data subjects must retain ultimate authorization over their data through an explicit, freely given, specific, and informed indication of their agreement before processing can commence. Furthermore, the principle of purpose limitation strictly prohibits data controllers from repurposing collected data for secondary objectives that are incompatible with the original, explicitly stated goals communicated to the data subject at the time of collection (Hoofnagle, van der Sloot, and Borgesius 2019).

Beyond the procedural management of data, the structural integrity of the protective framework relies heavily on the principles of data security and accountability. The principle of data security places a continuous, proactive obligation on data controllers and processors to implement state-of-the-art technical and organizational measures to safeguard personal information against unauthorized access, accidental alteration, or catastrophic data breaches. Complementing this technical requirement is the principle of accountability, which shifts the burden of proof directly onto the data controllers, legally binding them to demonstrate active compliance with all data protection standards and rendering them strictly liable for any institutional or systemic failures within their data processing pipeline. Together, these five core principles form an integrated regulatory lattice designed to maintain a balance of power between the individual data subject and high-capacity data processing entities.

The ultimate enforcement of these principles requires a sophisticated understanding of the relationship between data protection and criminal law, which functions through an essential dual-mechanism of preventive regulation and punitive enforcement. While administrative data protection frameworks excel at establishing proactive compliance metrics, auditing practices, and preventative security guidelines, they lack the raw deterrent capacity necessary to neutralize deliberate, malicious threat actors. Criminal

law steps into this regulatory vacuum by providing robust punitive enforcement mechanisms, transforming administrative non-compliance and malicious exfiltration into severe, punishable offenses characterized by custodial sentences and substantial corporate fines (Greenleaf 2023). Therefore, the criminalization of personal data violations does not replace preventative data governance; rather, it serves as the ultimate legislative sanction that gives teeth to regulatory oversight, ensuring that the digital identity and privacy of citizens are defended with the full coercive power of the state.

INDONESIAN LEGAL FRAMEWORK ON DIGITAL IDENTITY THEFT

The criminal law architecture governing digital identity theft in Indonesia is characterized by a multi-layered, evolving statutory framework that spans traditional codified law and modern cyber-specific legislation. Historically, the primary legal instruments utilized to combat identity-related offenses were anchored within the traditional Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana* or KUHP). Within this traditional framework, prosecutors frequently relied on fraud-related offenses, particularly Article 378 of the old KUHP (and its corresponding updated provisions in Law No. 1 of 2023), which criminalizes the act of deceiving individuals for illicit material gain through the assumption of a false name or a fraudulent status (Asshiddiqie 2022). However, this classical formulation of fraud possesses severe structural limitations when applied to the digital realm, as it inherently requires a direct, often interpersonal, deceptive interaction that results in immediate property transfer, thereby failing to capture the abstract, automated, and non-tangible dimensions of modern digital identity exfiltration.

To complement these traditional fraud provisions, the legal system relies on forgery and impersonation offenses historically codified under Article 263 of the KUHP concerning the falsification of physical documents. Legal scholars have noted that while identity theft frequently involves the creation of fraudulent credentials or the alteration of authentication tokens, traditional

forgery provisions are strictly bounded by a material requirement, meaning they are designed to protect the integrity of physical, signed documents rather than fluid digital data streams or cryptographic hashes (Marzuki 2021). Consequently, attempts by the judiciary to apply these analog articles to digital identity theft often necessitate expansive judicial interpretations that stretch the principle of legality (*asas legalitas*) to its conceptual limits (Butt 2021). This creates a state of jurisprudential instability, wherein the penalization of sophisticated digital impersonation remains contingent upon whether a court is willing to equate virtual profiles and binary code with physical instruments of deception.

Recognizing these statutory gaps, the Indonesian legislature enacted Law No. 11 of 2008 on Electronic Information and Transactions, which has undergone successive updates, most notably through Law No. 1 of 2024 (popularly known as the UU ITE). The UU ITE introduces specific cybercrime provisions designed to address the technical methodologies that precede and facilitate identity theft, most notably through its unauthorized access offenses. Article 30 of the UU ITE establishes strict criminal liability for any individual who deliberately and without right accesses another person's computer system or electronic infrastructure, effectively criminalizing the initial breach or hacking phase wherein personal data attributes are harvested (Sari and Ramli 2022). This provision serves as a critical statutory weapon, shifting the focus of criminal law from the retrospective damage caused by fraud to the proactive penalization of infrastructure compromise and illicit data reconnaissance.

In addition to unauthorized access, the UU ITE addresses the core actions of identity alteration through its comprehensive data manipulation offenses. Specifically, Article 35 of the UU ITE penalizes any individual who deliberately and without right creates, alters, deletes, or tampers with electronic information or electronic records with the intent that such data appear as if they were authentic. This particular provision is highly relevant to digital identity theft, as it captures the precise mechanism of synthetic identity creation, digital credential manipulation, and the forgery of digital signatures or authentication tokens (Suryono, Purwanto, and Setiawan 2023).

By establishing severe custodial sentences and corporate fines for data manipulation, the UU ITE creates a comprehensive cybercrime framework that attempts to decouple criminal liability from the physical constraints of the traditional KUHP, providing a more technologically neutral baseline for prosecuting sophisticated threat actors.

Furthemore, a fundamental paradigm shift occurred with the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP), which introduced a specialized, rights-based regime designed to safeguard individual informational autonomy. At the core of the UU PDP is the statutory codification of the rights of data subjects, which are explicitly designed to grant citizens complete control over their digital personas. These include comprehensive access rights, which allow individuals to demand verification regarding whether their data is being processed, and correction rights, which empower data subjects to rectify inaccuracies within institutional databases to prevent identity misattribution. Furthermore, the law establishes robust deletion rights, or the right to be forgotten, enabling individuals to demand the permanent erasure of their personal information when the legal basis for its processing has expired, thereby minimizing the lifetime availability of data pools vulnerable to identity thieves (Greenleaf 2023).

To operationalize these rights, the UU PDP imposes strict, legally binding obligations on data controllers, shifting the societal burden of cybersecurity from the individual citizen to high-capacity corporate and state institutions (Ramli et al. 2023). Among these duties, security obligations are paramount; data controllers must implement advanced technical and organizational measures, including encryption and pseudonymization, to shield stored data sets from external infiltration or internal leaks. Crucially, the UU PDP introduces strict breach notification requirements, mandating that in the event of a security failure that compromises personal data, the data controller must notify both the data subject and the regulatory authority within seventy-two hours. This notification mechanism is designed to mitigate the secondary impacts of identity theft, allowing individuals to immediately freeze their financial accounts and alter their access credentials

before threat actors can exploit the exfiltrated datasets.

The enforcement architecture of the UU PDP is further reinforced by a dual system of administrative and criminal sanctions, which together establish a highly punitive regulatory environment. On the administrative front, data protection authorities are empowered to issue severe compliance orders, freeze data processing activities, and levy administrative financial penalties for systemic compliance failures (Pramono and Utama 2024). Simultaneously, the criminal provisions of the UU PDP directly target the black market for personal information, establishing explicit criminal offenses for the illicit acquisition, collection, sale, and disclosure of personal data for personal or corporate enrichment. By imposing heavy custodial sentences that run concurrently with massive corporate penalties, the UU PDP transforms data protection from a passive administrative compliance checklist into a matter of high-stakes criminal liability (Simanjuntak and Elisabeth 2024).

The practical execution of these statutory mandates is distributed across a complex institutional framework comprising specialized state agencies and traditional law enforcement bodies. At the center of this ecosystem is the designated Data Protection Authority (DPA), which is mandated by the UU PDP to act as an independent regulatory referee overseeing compliance, issuing implementing regulations, and adjudicating administrative disputes between data subjects and controllers (Fanggidae 2024). The operationalization of this authority, however, requires constant structural coordination with national cybersecurity agencies, most notably the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN). The BSSN functions as the state's technical backbone, monitoring national network traffic, issuing threat intelligence reports, providing incident response protocols during critical data breaches, and ensuring that the technical infrastructure of both state e-government platforms and critical private sectors remains resilient against credential harvesting campaigns.

When administrative and technical preventions fail, the responsibility shifts to traditional law enforcement institutions, specifically the Indonesian National Police (*Kepolisian Negara Republik Indonesia* or Polri). Within the

organizational hierarchy of Polri, specialized units such as the Directorate of Cyber Crimes (*Direktorat Tindak Pidana Siber*) possess the primary mandate to investigate digital identity theft, execute digital forensics, track illicit cryptocurrency trails, and apprehend sophisticated cybercriminals (Pratama 2023). These police units operate in tandem with the Attorney General's Office (*Kejaksaan Agung*) and the commercial judiciary to navigate the complex evidentiary requirements inherent to cybercrime prosecution (Sulasno 2025). However, the operational efficacy of this institutional triad remains highly contingent upon continuous capacity-building, as the technical sophistication required to perform memory forensics, unpack obfuscated malware, and execute cross-border perpetrator attribution often outpaces the resource allocations of standard regional law enforcement divisions.

Despite the existence of these robust statutory frameworks and institutional actors, the Indonesian legal response to digital identity theft is severely undermined by the deep fragmentation of its existing regulations. This fragmentation manifests first as a web of overlapping provisions between the traditional KUHP, the cyber-centric UU ITE, and the specialized UU PDP (Siddiq 2024). Because all three statutes contain provisions that can simultaneously criminalize a single act of identity theft—such as evaluating the act under classical fraud, unauthorized system access, or illicit data acquisition—prosecutors frequently face immense confusion regarding which statutory pathway takes precedence. This multi-statutory overlap violates the principle of legal certainty and complicates the formulation of indictments, as different laws carry wildly disparate evidentiary thresholds, statutory definitions, and penal weights for fundamentally identical criminal behaviors.

This statutory overlap is further exacerbated by profound regulatory inconsistencies embedded within the text of the laws themselves. For instance, the definition of what constitutes valid electronic consent, the categorization of specific sensitive data types, and the standards for legal corporate liability differ significantly between the updated UU ITE and the newer UU PDP (Pramono and Utama 2024). These internal contradictions mean that an activity deemed legally compliant under one regulatory

framework can concurrently be interpreted as an actionable offense under another (Aspan 2023). These discrepancies cripple the compliance strategies of data controllers, who are forced to navigate an unstable regulatory environment where the legal goalposts are continuously shifted by uncoordinated amendments and conflicting ministerial regulations.

Ultimately, these overlaps and inconsistencies culminate in severe enforcement ambiguity across the entire justice system. Law enforcement officers on the ground are frequently left without clear guidance regarding which institutional body possesses primary jurisdiction over a specific data breach or identity theft incident, leading to systemic bureaucratic friction and delayed investigations (Wijaya and Santoso 2024). This ambiguity paralyzes the state's enforcement capacity, allowing agile cybercriminal networks to exploit the institutional vacuum created by turf wars and procedural inertia between regulatory agencies and police divisions. Without a unified, horizontally integrated judicial strategy that clearly reconciles the boundaries of each statute, the Indonesian legal framework remains structurally ill-equipped to mount a cohesive defense against the rising tide of digital identity theft (Utomo 2025).

CHALLENGES IN PROSECUTING DIGITAL IDENTITY THEFT

The primary hurdle in the criminal prosecution of digital identity theft inside the Indonesian judicial system centers on the technical complexity of perpetrator attribution. In the virtual environment, investigations are routinely obstructed by anonymous online actors who leverage advanced anonymizing infrastructures, such as the Onion Router (Tor) network and decentralized Virtual Private Networks (VPNs), to mask their routing signatures (Brenner 2021). These technologies effectively sever the direct digital link between a cybercriminal action and a physical individual. Consequently, law enforcement officers are frequently left with abstract internet protocol addresses that point to compromised proxy servers or commercial routers located in entirely different jurisdictions, preventing the establishment of the baseline identity required to issue criminal indictments

under the principle of individual criminal liability.

This attribution vacuum is further complicated by the systematic deployment of proxy identities and sophisticated social engineering techniques designed to confuse digital forensics units. Cybercriminals routinely purchase or lease bank accounts, digital wallets, and telecommunication profiles from complicit or identity-compromised third parties, known colloquially as "mules" (Levi 2020). When a digital identity theft or secondary financial fraud is executed, the digital footprint leads directly to these proxy individuals, who are often unaware of the scope of the criminal enterprise. This multi-layered obfuscation shifts the initial focus of police investigations onto innocent or low-level actors, draining state investigative resources and allowing the actual intellectual perpetrators behind the operations to remain insulated from state scrutiny.

Ultimately, these tactics are institutionalized by international cybercriminal networks that operate with corporate-level efficiency across multiple continents. These transnational syndicates intentionally fragment their operational infrastructure, launching identity exfiltration campaigns from one state, routing stolen datasets through cloud nodes in a second state, and laundering the financial proceeds in a third state (Zalnieriute 2021). This strategic structural fragmentation exploits the systemic limitations of domestic law enforcement agencies, which are bound by strict territorial sovereignty. As a result, when the Indonesian National Police attempt to track a coordinated credential harvesting ring, they quickly hit an informational wall, as the core criminal infrastructure sits completely beyond their domestic reach.

Once an identity theft operation is uncovered, prosecutors face severe structural obstacles regarding the collection of digital evidence. Unlike physical evidence, digital information is characterized by extreme volatility, meaning it can be altered, overwritten, or permanently destroyed remotely within fractions of a second. Data preservation challenges are heightened by the widespread adoption of ephemeral messaging applications and automated system logs that overwrite themselves every few days (Pratama 2023). If regional police investigators fail to immediately issue formal

preservation orders to service providers or execute forensic imaging of compromised devices, critical metadata—such as session tokens, access timestamps, and communication logs—is lost forever, crippling the evidentiary foundation of the case before it reaches a courtroom.

Even when digital evidence is successfully preserved, verifying its authenticity and integrity presents a severe hurdle during judicial adjudication. Under the Indonesian Electronic Information and Transactions Law (UU ITE), digital evidence must be proved to have remained unaltered throughout the entire chain of custody, from initial seizure to court presentation. This verification requirement demands the application of strict cryptographic hashing algorithms and continuous forensic logging (Suryono, Purwanto, and Setiawan 2023). However, defense counsels routinely exploit minor gaps in the forensic chain of custody, arguing that the fluid and malleable nature of electronic files leaves them vulnerable to external manipulation, planting, or unauthorized modification, thereby raising reasonable doubt in the mind of the judiciary.

These technical verification hurdles are further compounded by strict admissibility concerns established by the formal criminal procedure code. Indonesian courts maintain highly rigid procedural compliance standards regarding how electronic materials must be retrieved and presented. For instance, if an investigator extracts a chat log or a database registry from a suspect's smartphone without a specific, prior judicial warrant—even under emergency circumstances involving active data deletion—the court may rule the entire dataset inadmissible as fruit of the poisonous tree. This procedural rigidity often creates a sharp conflict between the rapid, fluid demands of digital forensics and the slow, document-heavy requirements of traditional criminal procedure law, forcing prosecutors to abandon critical evidence due to minor administrative infractions.

The prosecution of digital identity theft in the modern era is fundamentally constrained by cross-border data challenges, primarily driven by the ubiquity of foreign data storage. The vast majority of digital platforms, e-commerce giants, and social media networks utilized by Indonesian citizens are operated by multinational conglomerates that host their physical data

repositories within foreign jurisdictions, such as the United States or the European Union (Greenleaf 2023). When an identity breach occurs, the critical access logs and account data required to prove a suspect's guilt reside on servers outside Indonesian territory. Consequently, domestic investigators cannot execute standard search and seizure warrants, leaving them completely dependent on international cooperation frameworks that are notoriously slow and politically complex.

This problem is exacerbated by the architecture of modern cloud computing environments, where personal data is no longer stored on a singular, identifiable physical drive. Instead, cloud infrastructures utilize dynamic distributed storage systems, meaning an individual's digital identity attributes are fragmented, encrypted, and continuously shifted across multiple server farms globally to optimize network performance (Hoofnagle, van der Sloot, and Borgesius 2019). This fluid redistribution makes it technically impossible for local law enforcement to pinpoint the exact physical location of the evidence. This spatial ambiguity alienates traditional legal doctrines that require precise geographic identification for search warrants, rendering standard investigative tools obsolete against cloud-native cybercriminals.

These technical realities culminate in severe jurisdictional conflicts that paralyze transnational cybercrime prosecutions. When Indonesian authorities attempt to retrieve data from foreign tech companies, they encounter profound legal contradictions, such as when foreign privacy laws, like the European Union's GDPR, strictly prohibit the disclosure of personal data to foreign police forces without explicit treaty authorizations (Simanjuntak and Elisabeth 2024). This friction turns a standard criminal investigation into a diplomatic stand-off. Because the formal Mutual Legal Assistance (MLA) process regularly takes months or even years to execute, the volatile digital evidence in question often expires or is scrubed by the hosting company long before the legal paperwork is cleared, creating a structural shield of impunity for international hackers.

On a domestic level, the systemic enforcement of identity theft regulations is deeply restricted by limited cyber forensic expertise across the

broader Indonesian law enforcement apparatus. While specialized elite divisions, such as the Police Cyber Crime Directorate in Jakarta, possess high-level technical competencies, the vast majority of regional and local police stations (*Polres* and *Polsek*) lack trained personnel capable of handling complex digital forensics (Pratama 2023). Local investigators frequently struggle with basic electronic evidence collection, missing volatile data stored in random-access memory (RAM) or failing to isolate seized devices from network signals, which frequently allows suspects to initiate remote factory resets that erase all incriminating data.

This expertise deficit is a direct consequence of severe resource constraints that afflict public sector judicial institutions. Maintaining a state-of-the-art digital forensics laboratory requires continuous, capital-intensive investments in specialized software licenses, high-performance computing hardware, and advanced decryption tools. Given the state's competing fiscal priorities, many regional prosecution offices and police stations operate with outdated technical equipment that cannot bypass modern hardware encryption or analyze complex blockchain transactions used in ransom schemes (Sulasno 2025). This technological gap creates an asymmetry of capabilities, wherein under-resourced state investigators are structurally outmatched by highly profitable cybercriminal syndicates that utilize cutting-edge evasion tools.

Finally, these institutional vulnerabilities are maximized by persistent inter-agency coordination issues that fracture the state's defensive front. The responsibility for securing Indonesia's digital identity ecosystem is divided among a patchwork of institutions, including the National Police, the Ministry of Communication and Digital Economy, the National Cyber and Crypto Agency (BSSN), and the newly formed Data Protection Authority (Pramono and Utama 2024). Due to overlapping mandates, a distinct lack of centralized data-sharing platforms, and bureaucratic turf protection, these entities often operate in isolation, failing to share real-time threat intelligence or forensic insights. This institutional siloization delays response times during massive data breaches, allowing identity thieves to systematically exploit the bureaucratic friction between state agencies to exfiltrate and

monetize the personal data of millions of citizens before a coordinated defense can be mounted.

COMPARATIVE ANALYSIS OF INTERNATIONAL APPROACHES

European Union

The global benchmark for data privacy and identity protection is anchored within the European Union's General Data Protection Regulation (GDPR), which establishes a highly comprehensive data protection framework. Unlike sector-specific privacy regimes, the GDPR applies a unified, extra-territorial omni-broad standard that covers all public and private entities processing the personal data of EU residents (Hoofnagle, van der Sloot, and Borgesius 2019). This statutory uniformity eliminates the regulatory fragmentation that frequently cripples developing legal systems. By establishing a single, coherent legislative text, the EU ensures complete legal certainty, preventing threat actors from exploiting jurisdictional or statutory loopholes between overlapping national laws.

Central to the success of the GDPR is its robust codification of enforceable data subject rights, which are designed to protect the integrity of the digital persona. These rights include the right to data portability, the right to object to automated profiling, and the right to immediate erasure, which together empower individuals to actively police their own digital footprint (Floridi 2020). By legally forcing data controllers to facilitate these rights through accessible user interfaces, the GDPR reduces the systemic availability of stale or unmonitored personal data pools. This active minimization of data exposure directly correlates with a reduction in the raw material available to cybercriminals for weaponization in credential stuffing or synthetic identity campaigns.

Furthermore, the European framework derives its immense deterrent capability from its severe and uncompromising enforcement mechanisms. Independent data protection authorities across EU member states are empowered to levy catastrophic administrative fines of up to twenty million euros or four percent of a corporate entity's global annual turnover for

systemic security or compliance failures (Zalnieriute 2021). This punitive framework forces corporate boards to elevate cybersecurity from a peripheral technical concern to a matter of existential financial survival. Consequently, private entities invest heavily in proactive data protection architectures, creating a resilient corporate defense infrastructure that dramatically limits the success rate of external identity exfiltration attempts.

Singapore

In contrast to the rights-centric European model, Singapore utilizes a highly pragmatic, market-friendly personal data governance model via its Personal Data Protection Act (PDPA). The Singaporean framework acknowledges the economic necessity of data flows, balancing the protection of personal data with the legitimate operational needs of commercial enterprises (Greenleaf 2023). However, this flexible approach is backed by rigorous data intermediary regulations, meaning that corporations remain strictly liable for the security practices of any third-party contractors or cloud service providers they engage. This strict downstream accountability ensures that the outsourcing of data processing does not create weak points in the data security pipeline that could be exploited by identity thieves.

To complement this regulatory model, Singapore has deployed highly coordinated cybercrime enforcement strategies through its specialized Computer Misuse Act (CMA). The CMA directly penalizes the technical precursors of identity theft, establishing severe criminal penalties for unauthorized access to computer materials, interception of network services, and the use of stolen encryption keys. Singapore's enforcement efficacy is maximized by the centralized architecture of its cyber defense, where the Cyber Security Agency (CSA) acts as a single national coordinator bridging the gap between private enterprise, financial institutions, and specialized police units. This unified operational loop allows for real-time data-sharing and rapid perpetrator attribution during active network intrusions.

Malaysia

Within the Southeast Asian region, Malaysia offers an instructive regulatory template through its Personal Data Protection Act (PDPA) 2010. The Malaysian statute represents an early regional attempt to institutionalize core data protection principles within a developing digital economy, explicitly targeting commercial transactions. The Malaysian framework applies a set of strict processing principles that place a heavy emphasis on security, disclosure, and data retention standards (Greenleaf 2023). By explicitly prohibiting the indefinite storage of consumer data, the Malaysian PDPA limits the lifetime risk of data breach exploitation, forcing corporations to systematically purge historical records that are no longer strictly necessary for active business operations.

The operational execution of this regime is structurally supported by specialized institutional enforcement structures under the Ministry of Digital. Malaysia utilizes a dedicated Personal Data Protection Commissioner who possesses broad inspection, enforcement, and investigative powers to police corporate compliance. While the Malaysian model has historically faced criticisms regarding its exclusion of the public sector from data privacy mandates, its centralized regulatory approach provides a clear institutional hierarchy that avoids the bureaucratic friction and turf wars often seen in states with overlapping regulatory jurisdictions. This clear division of administrative labor facilitates smoother corporate auditing and quicker deployment of regulatory sanctions following a data compromise event.

United States

The United States approaches digital identity theft through a highly decentralized, sector-specific legal framework characterized by specialized identity theft legislation at both the federal and state levels. At the federal core is the Identity Theft and Assumption Deterrence Act, which explicitly criminalizes the transfer, possession, or use of another person's identification details with the intent to commit unlawful activities. This legislation is unique because it formally recognizes the individual victim of identity theft as a direct injured party entitled to mandatory financial restitution, a critical

judicial dimension that shifts the focus of criminal outcomes toward victim remediation and economic restoration (Levi 2020).

To enforce these statutes, the American legal system utilizes highly specialized criminal enforcement mechanisms designed to overcome the technical challenges of modern cybercrime. Agencies such as the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC) operate dedicated cyber task forces that integrate forensic accountants, data engineers, and federal prosecutors into singular investigative units. These units are legally empowered by comprehensive electronic surveillance statutes, such as the Stored Communications Act, which allow for the rapid preservation and retrieval of volatile digital evidence from telecommunication providers. Furthermore, the US aggressively utilizes corporate liability doctrines, prosecuting financial institutions that fail to maintain adequate "Red Flags Rule" identity verification procedures, thereby cutting off the commercial pathways through which stolen identities are monetized.

Lessons for Indonesia

The comparative analysis of these international frameworks provides critical, actionable lessons for the structural reform of the Indonesian legal system, beginning with the absolute necessity of creating harmonized regulatory frameworks. Indonesia must aggressively reconcile the statutory contradictions and overlapping provisions currently existing between its traditional Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the newly enacted Personal Data Protection Law (UU PDP) (Pramono and Utama 2024). By adopting the EU's model of unified, non-fragmented statutory standards and the US approach to clear criminal definitions, the Indonesian legislature can eliminate the legal uncertainty that currently complicates the formulation of criminal indictments and paralyzes regional investigators.

Secondly, the international experience highlights that statutory laws are entirely useless without strong institutional oversight characterized by complete regulatory independence and high technical capacity. Drawing

from the models of Singapore's CSA and the European DPAs, Indonesia must ensure that its newly established Data Protection Authority is granted full financial, political, and operational autonomy from executive ministries (Fanggidae 2024). This independent authority must be equipped with centralized enforcement mandates, enabling it to issue binding compliance penalties against both private corporations and state ministries without navigating bureaucratic hurdles, thereby ending the institutional siloization that currently cripples national cybersecurity responses.

Finally, Indonesia must structurally overhaul its judicial machinery to implement effective enforcement models capable of addressing the modern cybercrime lifecycle. This requires moving away from archaic, localized policing methods toward the institutionalization of specialized cyber-prosecution units and dedicated digital forensic laboratories across all regional police commands (Pratama 2023). In tandem, the legislature must update the formal Criminal Procedure Code (KUHP) to adopt the flexible, rapid digital evidence preservation standards utilized in the United States and Singapore, while simultaneously integrating mandatory victim restitution clauses into national cybercrime sentencing guidelines (Sulasno 2025). Only by synthesizing these global best practices into a coherent, horizontally integrated national strategy can Indonesia build a legal infrastructure resilient enough to dismantle transnational cybercriminal networks and protect the digital sovereignty of its citizens.

DIGITAL IDENTITY THEFT AND EMERGING CYBERSECURITY RISKS

The contemporary crisis of digital identity theft is structurally inextricably linked to the escalating frequency and scale of corporate and state data breaches, which act as systemic catalysts for subsequent identity-related crimes. Large-scale personal data leaks from centralized storage systems remove the necessity for cybercriminals to target individual users directly. Instead, malicious actors infiltrate single high-capacity repositories—such as those maintained by e-commerce giants, telecommunication firms, or insurance agencies—to exfiltrate the combined credentials of millions of

citizens simultaneously (Zalnieriute 2021). These massive security breaches flood the illicit digital economy with structured personal datasets, significantly reducing the cost and effort required for threat actors to acquire valid target information.

Once these personal datasets are exfiltrated, they undergo a systematic process of secondary criminal exploitation on dark web marketplaces and encrypted communication networks. Criminal syndicates deploy automated data-parsing algorithms to clean, cross-reference, and index the leaked data, transforming disorganized raw text into highly actionable consumer dossiers. This aggregated data is then monetized as a specialized commodity, sold to lower-level cybercriminals who specialize in targeted exploitation tactics (Bany Mohammed et al. 2023). The availability of these pre-compiled identity packages creates a perpetual loop of secondary offenses, ensuring that a single corporate data breach can fuel localized fraud operations, phishing campaigns, and credential-stuffing attacks for several years after the initial infrastructure compromise occurs.

The threat landscape of identity theft has experienced a profound technical evolution due to the rapid integration of advanced artificial intelligence, which has radically augmented the capabilities of modern cybercriminals. Chief among these technological shifts is the proliferation of sophisticated deepfake technologies, which utilize deep generative adversarial networks to synthesize highly realistic video, image, and voice modulations of target individuals. In the context of identity fraud, deepfakes allow attackers to bypass biometric authentication systems—such as facial recognition nodes and voice verification protocols—that are widely deployed by financial and administrative institutions to secure user accounts (Levi 2020). By simulating a victim's physical presence with absolute precision, cybercriminals can undermine the foundational premise of modern identity verification.

Furthermore, the deployment of AI-generated impersonation schemes has fundamentally transformed the scale and efficacy of social engineering campaigns. Threat actors utilize large language models to automate the generation of highly personalized, context-aware phishing communications

that mirror the specific linguistic style, professional terminology, and structural formatting of trusted entities or personal acquaintances. These AI-driven systems can analyze vast amounts of open-source intelligence harvested from a victim's public social media presence to draft tailored deceptive narratives at scale (Bany Mohammed et al. 2023). By eliminating the grammatical errors and structural inconsistencies that historically characterized automated fraud, AI-generated impersonation maximizes cognitive manipulation, resulting in significantly higher success rates for credential harvesting campaigns.

The rapid expansion of the financial technology (FinTech) sector has created an expansive, highly vulnerable target area for identity thieves, particularly within modern digital banking infrastructures. As traditional banking models migrate toward mobile-first, branchless architectures, the identity verification processes governing account creation and transaction authorization have become entirely automated. Cybercriminals exploit structural vulnerabilities within these digital onboarding frameworks, utilizing compromised credentials or synthetic identity profiles to open unauthorized banking accounts (Suryono, Purwanto, and Setiawan 2023). These fraudulent accounts are then used as operational channels to execute complex money laundering schemes, store stolen funds, and launch secondary financial crimes, while insulating the actual perpetrators from regulatory tracing.

Simultaneously, the pervasive adoption of e-wallet applications has introduced new vectors for systemic e-wallet abuse and account takeover fraud. Because e-wallets prioritize transaction speed and user convenience, they frequently employ less stringent multi-factor authentication requirements compared to institutional banking apps. Attackers exploit this design preference through SIM-swapping maneuvers or credential harvesting, allowing them to hijack a victim's e-wallet profile and drain linked credit cards or bank balances within minutes (Levi 2020). The automated speed of these transactions makes real-time fraud mitigation extremely difficult for operators, leaving victims with immediate financial liabilities before the unauthorized access is even detected by system anomaly

logs.

This financial risk is further amplified by the emergence of online lending platforms, which have become a primary target for identity exploitation due to their low-friction credit allocation models. Peer-to-peer lending applications frequently utilize rapid machine learning algorithms to evaluate credit applications within minutes, requiring only a digital upload of a national identification card and a basic portrait photograph. Identity thieves weaponize this operational speed by submitting stolen or manipulated identification materials to secure instant unsecured loans under a victim's name (Suryono, Purwanto, and Setiawan 2023). By the time the credit institution attempts to collect on the defaulted loan, the innocent data subject is already facing severe financial blacklisting and profound credit score degradation, exposing a critical lack of structural verification coordination between alternative lenders and centralized credit bureaus.

Beyond the commercial marketplace, the digitization of public sectors has introduced severe systemic risks within electronic government (e-government) systems. Modern states increasingly consolidate public health registries, civil taxation records, and social welfare distribution mechanisms into centralized, cloud-hosted digital architectures to optimize administrative efficiency (Sari and Ramli 2022). However, this high concentration of sensitive citizen data creates a high-value target for state-sponsored threat actors and international cybercriminal organizations. When an e-government platform suffers an identity breach, the compromised data points—such as tax identification numbers, family registry details, and military records—cannot be easily changed or reset like a commercial password, resulting in permanent vulnerability for the affected population.

Ultimately, these architectural vulnerabilities pose a direct threat to the structural integrity of national digital identity programs. When a state mandates a single, centralized digital credential or biometric passport to regulate access to all public and private services, that digital identity becomes a single point of failure for the entire nation (Hoofnagle, van der Sloot, and Borgesius 2019). If an advanced persistent threat group succeeds in compromising the root authentication keys of a national identity program,

they gain the capacity to execute widespread identity theft, forge state documentation, manipulate voting registries, and gain unauthorized entry into critical national infrastructure. Consequently, the failure to secure public sector identity ecosystems goes beyond standard consumer privacy concerns, directly threatening the national security, economic stability, and digital sovereignty of the state.

STRENGTHENING CRIMINAL PROTECTION OF PERSONAL DATA

The development of a resilient defense infrastructure against cyber-enabled impersonation requires immediate, structural regulatory harmonization between existing cybercrime regulations and data protection laws. Within the Indonesian context, this requires a systematic reconciliation of the statutory overlaps and conceptual frictions currently existing between the traditional Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Personal Data Protection Law (UU PDP) (Siddiq 2024). Legislators must provide an explicit clarification of offenses, drawing bright lines between simple administrative data non-compliance, active data exfiltration, and downstream identity deployment. This statutory mapping is essential to eliminate the judicial confusion that currently plagues the drafting of criminal indictments and prevents multi-statutory double jeopardy complications.

Furthermore, this legislative realignment must introduce consistent sanctions across all interconnected statutes to ensure proportional and uniform sentencing outcomes. Currently, the legal system features a disjointed distribution of penalties, where fundamentally identical criminal behaviors—such as the unauthorized harvesting of personal identifiers—carry wildly disparate fines and custodial sentences depending on whether a prosecutor charges the suspect under the UU ITE or the UU PDP (Pramono and Utama 2024). By anchoring criminal fines to a standard economic loss matrix and standardizing corporate liability triggers across all active statutes, the state can project a uniform deterrent signal. This regulatory coherence ensures that criminal networks cannot locate and exploit soft spots or low-

penalty pathways within the national sentencing framework.

Ultimately, these harmonized standards must culminate in a comprehensive identity theft regulation that formally establishes a specific criminal categorization for identity offenses. Rather than treating identity theft as an ancillary or derivative element of general fraud or computer hacking, the legislature must codify it as an independent, standalone felony that attacks the integrity of the digital persona (Koops et al. 2013). This dedicated classification must be paired with enhanced victim protection mechanisms, shifting the focus of the criminal justice system from state-centric penalties to individual restoration. This includes enacting mandatory statutory clauses that facilitate rapid identity restoration certificates, protect victims from wrongful debt enforcement by alternative financial lenders, and provide automatic clearing mechanisms for secondary criminal records erroneously attributed to the compromised data subject.

The practical enforcement of a harmonized legal framework is entirely dependent on the operational capacity of specialized cybercrime units within the state's law enforcement apparatus. The Indonesian National Police must structurally scale the organizational footprint of the Directorate of Cyber Crimes from centralized federal commands down to all regional and provincial law enforcement divisions (Pratama 2023). These regional divisions must be decoupled from traditional property crime units, transforming them into specialized tactical commands capable of tracking fluid digital footprints. By institutionalizing these dedicated units, the state ensures that local investigators are equipped with the specialized mandates required to intercept active credential harvesting nodes before they scale into national data breach disasters.

Simultaneously, the state must establish dedicated data protection enforcement mechanisms within the independent Data Protection Authority (DPA) mandated by the UU PDP. This regulatory body must not function merely as an administrative auditing agency; it must be equipped with independent investigative powers, including the authority to execute unannounced compliance raids, subpoena system architecture logs from corporate entities, and issue binding data-freezing orders (Fanggidae 2024).

To prevent the bureaucratic turf wars that traditionally cripple inter-agency law enforcement, a formalized joint operational protocol must be established between the DPA, the National Cyber and Crypto Agency (BSSN), and the cyber divisions of the police. This integrated coordination model ensures that technical asset discovery, administrative data auditing, and criminal apprehension occur simultaneously during a critical infrastructure compromise event.

To match the technical sophistication of modern transnational cybercriminal syndicates, the state must execute an aggressive nationwide investment campaign in digital forensic capacity building. Law enforcement laboratories must be systematically equipped with advanced forensic tools capable of executing volatile memory forensics, bypassing complex hardware-level encryption, and de-anonymizing multi-layered proxy networks (Pratama 2023). This technological acquisition must specifically target artificial intelligence-driven forensic software capable of identifying deepfake image manipulation and mapping obfuscated blockchain transactions used by identity syndicates to launder the proceeds of synthetic credit fraud.

The deployment of advanced hardware must be paired with continuous, institutionalized investigator training programs developed in partnership with leading global cybersecurity institutes and academic entities. Police officers, state prosecutors, and members of the judiciary must undergo rigorous technical training to comprehend the mechanics of automated credential stuffing, API security vulnerabilities, and asymmetric cryptographic signatures (Sulasno 2025). This capacity building is critical to bridge the acute expertise gap currently existing between under-resourced public investigators and highly profitable private hackers. Ensuring that judges possess a high degree of digital literacy prevents the dismissal of valid circumstantial electronic evidence due to an institutional misunderstanding of digital system dynamics.

Furthermore, the integrity of the judicial process relies heavily on the modernization of digital evidence management systems to protect the chain of custody. The state must deploy decentralized, immutable digital evidence

ledgers—potentially utilizing blockchain architectures—to log every access, transmission, and analysis phase executed on seized electronic materials (Suryono, Purwanto, and Setiawan 2023). This systematic logging is vital to satisfy the strict integrity and authenticity verification requirements enforced by Article 5 and Article 6 of the UU ITE. By eliminating the risk of internal database tampering or accidental file alteration within police storage units, these secure management systems protect the admissibility of volatile digital evidence from aggressive defense challenges during formal court proceedings.

Given that digital identity theft operates almost exclusively across transnational cyber infrastructures, domestic prosecution models will remain structurally ineffective without deep integration into international cooperation networks. Indonesia must move toward formal accession to international cybercrime standards, most notably the Budapest Convention on Cybercrime, to align its domestic procedural laws with global benchmarks (Sulasno 2025). Accession to such frameworks provides a standardized vocabulary and legal infrastructure that facilitates rapid, borderless cross-border investigations. This integration prevents international threat actors from using jurisdictional differences to escape prosecution.

To operationalize this global integration, the state must establish real-time information-sharing mechanisms with international law enforcement networks, including Interpol's cybercrime divisions and foreign national computer emergency response teams (CERTs). These collaborative channels must bypass traditional, document-heavy diplomatic pathways to facilitate the rapid transmission of active threat intelligence, server access logs, and malicious IP registries (Brenner 2021). By building these secure data-sharing networks, the Indonesian National Police can execute synchronized containment strategies with foreign counterparts, freezing international proxy nodes and capturing threat actors simultaneously before they can purge their remote storage infrastructures.

Finally, these proactive networks must be legally supported by streamlined mutual legal assistance (MLA) procedures that are explicitly optimized for the speed of electronic data retrieval. The state must negotiate

specialized bilateral and multilateral electronic MLA treaties that reduce data preservation and retrieval processing times from months to hours (Simanjuntak and Elisabeth 2024). These modernized treaties must force foreign cloud service providers and multinational digital platforms to respect domestic data preservation requests under reciprocal enforcement agreements. By cutting through the geopolitical friction that traditionally stalls transnational evidence gathering, these streamlined MLA procedures ensure that volatile data registries are legally secured before they expire or are permanently scrubbed by automated system management protocols.

While punitive enforcement and technical capacity building form the defensive armor of the state, the long-term containment of digital identity theft requires a fundamental elevation of societal resilience through targeted public awareness and prevention strategies. The state must design and execute comprehensive digital literacy programs integrated directly into national educational curricula across primary, secondary, and higher education levels (Sari and Ramli 2022). These educational modules must move beyond basic functional computer literacy to cultivate deep critical thinking competencies regarding data privacy, explaining the mechanics of social engineering, the dangers of digital over-sharing, and the value of personal informational self-determination.

These systemic educational updates must be supported by continuous, high-visibility cybersecurity awareness campaigns executed in partnership with civil society organizations, mass media networks, and private telecommunication providers. These campaigns must utilize dynamic, multi-platform media distributions to inform the general public regarding immediate tactical threat indicators, such as identifying advanced spear-phishing signatures, managing complex passwords via decentralized managers, and the mandatory deployment of multi-factor authentication protocols (Bany Mohammed et al. 2023). By transforming cybersecurity from an abstract corporate concern into an accessible daily civic habit, these public campaigns systematically reduce the vulnerability of the human element, which remains the primary entry point exploited by identity thieves.

Ultimately, these initiatives must converge into a continuous national

personal data protection education infrastructure directed at small-and-medium enterprises (SMEs) and localized digital public services. Because these lower-tier market participants handle immense volumes of consumer data but lack the capital-intensive security architectures of multinational corporations, they represent high-vulnerability targets for identity theft rings (Suryono, Purwanto, and Setiawan 2023). The state, via the DPA and the Ministry of Communication and Digital Economy, must distribute accessible, open-source data compliance toolkits, conduct subsidized data protection officer certifications, and establish localized security audit networks. By elevating the baseline operational security practices of the entire commercial ecosystem, Indonesia can transition from a reactive, damage-mitigation model to a proactive, highly resilient data protection posture that effectively safeguards the digital sovereignty of its citizens.

CONCLUSION

The escalation of digital identity theft in Indonesia presents a structural challenge that exposes critical vulnerabilities within the nation's legal and institutional architecture. While the enactment of the Personal Data Protection Law (UU PDP) marks a significant step forward, its integration with existing legislation, such as the Electronic Information and Transactions Law (UU ITE) and the traditional Criminal Code (KUHP), remains heavily fragmented. This regulatory fragmentation, coupled with systemic challenges in digital perpetrator attribution, evidence preservation, and jurisdictional boundaries, creates an environment where cybercriminals can operate with a high degree of impunity. To secure its digital economy, Indonesia must move away from isolated, reactive enforcement strategies toward a unified approach that treats digital identity as a fundamental component of human dignity and national security.

Ultimately, resolving these systemic vulnerabilities requires an aggressive legal and structural overhaul modeled after global best practices. The Indonesian government must prioritize the absolute operational independence of the newly established Data Protection Authority (DPA) and

ensure seamless coordination with specialized cybercrime divisions and national cybersecurity bodies. Furthermore, the state must make long-term investments in digital forensics infrastructure, modernize electronic mutual legal assistance procedures for rapid cross-border investigations, and integrate comprehensive digital privacy education into public awareness campaigns. By building a cohesive and unified legal framework that bridges the gap between proactive data governance and swift criminal prosecution, Indonesia can establish a resilient digital ecosystem capable of safeguarding its citizens' data sovereignty.

ACKNOWLEDGMENTS

None.

FUNDING INFORMATION

None.

CONFLICTING INTEREST AND ORGINALITY STATEMENT

The authors state that there is no conflict of interest in the publication of this article.

GENERATIVE AI STATEMENT

None.

REFERENCES

Aspan, Henry. 2023. "Harmonization of Cyber Law and Personal Data Protection in Indonesia: Facing the Dilemma of Overlapping Sanctions." *Journal of ASEAN Law and Policy* 11 (2): 112–129.

Asshiddiqie, Jimly. 2022. *Constitutional Law and Cyber-Jurisprudence in the Digital Era*. Jakarta: Rajawali Pers.

Bany Mohammed, Ahmad, Ashwaq Al-Amiri, Omar Al-Hazaimeh, and Mahmoud Al-Khasawneh. 2023. "The Escalation of Digital Identity Theft

in E-Commerce: A Multidisciplinary Review of Cybercrime Tactics." *Journal of Cyber Security and Data Governance* 12 (2): 145–167.

Brenner, Susan W. 2021. *Cybercrime: Criminal Threats in the Information Age*. San Francisco: Law and Technology Press.

Butt, Simon. 2021. "The Principle of Legality and Judicial Interpretation in Indonesian Criminal Law." *Asian Journal of Comparative Law* 16 (1): 34–56. https://doi.org/10.1017/asjcl.2021.5.

Bygrave, Lee A. 2020. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Fanggidae, Robert. 2024. "The Role of the New Data Protection Authority under the Indonesian PDP Act: Independent or Subordinate?" *Constitutional Review* 10 (1): 78–99. https://doi.org/10.31078/consrev1014.

Floridi, Luciano. 2020. "The Fight for Informational Privacy: Self-Determination in a Hyperconnected World." *Philosophy & Technology* 33 (1): 1–9. https://doi.org/10.1007/s13347-020-00393-y.

Floridi, Luciano. 2020. "The Fight for Informational Privacy: Self-Determination in a Hyperconnected World." *Philosophy & Technology* 33 (1): 1–9. https://doi.org/10.1007/s13347-020-00393-y.

Greenleaf, Graham. 2023. *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford: Oxford University Press.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 2019. "The European General Data Protection Regulation: What it is and What it Means." *Information & Communications Technology Law* 28 (1): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Koops, Bert-Jaap, Ronald Leenes, Paul de Hert, and Silvia De Conca. 2013. "Identity Theft and Fraud: Crime Typologies and Legislative Responses." *Computer Law & Security Review* 29 (4): 344–355.

Levi, Michael. 2020. "The Cyber-Identity Theft Nexus: Financial Losses, Reputational Harms, and the Architecture of Online Fraud." *Criminology & Public Policy* 19 (3): 821–845.

Marzuki, Peter Mahmud. 2021. *Penelitian Hukum: Edisi Revisi*. Jakarta: Prenada Media Group.

Pramono, Budi, and Widya Utama. 2024. "Enforcement Challenges of the

New Indonesian Personal Data Protection Act: Institutional Redundancy and Technical Obstacles." *Indonesia Law Review* 14 (1): 45–62.

Pratama, Rio. 2023. "Digital Forensics and Cybercrime Investigation Challenges in the Indonesian National Police Force." *Journal of Forensic and Digital Evidence* 5 (2): 143–159.

Ramli, Ahmad M., Tasya Safiranita, Keri Lestari, and Intan Nurrahma. 2023. "Corporate Obligations and Liabilities of Data Controllers under the Indonesian Personal Data Protection Act." *Padjadjaran Journal of Law* 10 (1): 12–31. https://doi.org/10.22304/pjih.v10n1.a1.

Sari, Indah, and Ahmad M. Ramli. 2022. "Digital Transformation and Cyber Vulnerabilities in Indonesian E-Government and E-Commerce Sectors." *Padjadjaran Journal of Law* 9 (2): 201–219.

Siddiq, Muhammad. 2024. "Regulatory Overlaps in Indonesian Cyberlaw: A Doctrinal Analysis of the ITE Law and the PDP Law." *Mimbar Hukum* 36 (1): 88–107. https://doi.org/10.22146/jmh.v36i1.9213.

Simanjuntak, Enrico, and Maria Elisabeth. 2024. "Criminalization of Personal Data Misuse: A Comparative Study of Indonesia's PDP Law and the European GDPR." *Indonesian Journal of International Law* 21 (2): 215–240.

Solove, Daniel J. 2024. *Understanding Privacy*. Cambridge: Harvard University Press.

Sulasno, Heri. 2025. "Cross-Border Cybercrime Investigation and Digital Evidence Attribution under Indonesian Law." *Journal of Indonesian Legal Studies* 10 (1): 89–114. https://doi.org/10.15294/jils.v10i1.73412.

Suryno, Ryan Randy, Purwanto Purwanto, and Budi Setiawan. 2023. "Data Manipulation and Digital Forgery under the Amended Indonesian E-Commerce and ITE Laws." *Journal of Theoretical and Applied Information Technology* 101 (14): 5601–5615.

Suryono, Ryan Randy, Purwanto Purwanto, and Budi Setiawan. 2023. "Data Manipulation and Digital Forgery under the Amended Indonesian E-Commerce and ITE Laws." *Journal of Theoretical and Applied Information Technology* 101 (14): 5601–5615.

Utomo, Tri Widodo W. 2025. "Institutional Redundancy and Bureaucratic Inertia in Safeguarding Indonesia's Cyberspace." *Journal of Public*

Administration and Governance in Asia 7 (1): 45–67.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Wijaya, Andy, and Budi Santoso. 2024. "Enforcement Ambiguity in Digital Identity Theft Cases: The Dilemma of Regional Investigators in Indonesia." *Lex Jurnalica* 21 (3): 310–328.

Windley, Phillip J. 2005. *Digital Identity: Unmasking the Website and Users Behind the Screen*. Sebastopol: O'Reilly Media.

Zalnieriute, Monika. 2021. "The Global Economy of Personal Data: Cybercrime, Commodification, and the Limits of Data Protection Law." *International Data Privacy Law* 11 (3): 223–239. https://doi.org/10.1093/idpl/ipab011.

This page is inteionally left blank