Journal of International Trade, Logistics and Law, Vol. 12, Num. 1, 2026, 259-270

ONLINE GAMBLING NETWORKS AND THE COMMODIFICATION OF PERSONAL DATA: ADDRESSING THE INEVITABILITY OF DATA BREACHES

Michelle Priscilla KESUMA
Universitas Pelita Harapan, Indonesia

Fajar SUGIANTO
Universitas Pelita Harapan, Indonesia

Vincensia Esti P SARI
Universitas Pelita Harapan, Indonesia

Velliana TANAYA
Universitas Pelita Harapan, Indonesia

Jerry SHALMONT
Universitas Pelita Harapan, Indonesia

Received: March 06, 2026 Accepted: May 26, 2026 Published: June 01, 2026

Abstract:
This research investigates the legal standing and protection of personal data subjects within the Indonesian digital landscape, specifically addressing the escalating risks of data commodification and its exploitation by the illegal online gambling industry. Adopting a normative legal research methodology with a statutory and conceptual approach, this study analyzes primary and secondary legal materials, including the Indonesian PDP Law and international frameworks such as the GDPR. By synthesizing Shoshana Zuboff's theory of surveillance capitalism with Soerjono Soekanto's legal effectiveness framework, this study exposes a profound structural asymmetry between data controllers and subjects. The analysis reveals that while the Law of the Republic of Indonesia Number 27 of 2022 (PDP Law) provides a robust normative foundation, its practical efficacy is severely hampered by institutional unreadiness, forensic gaps, and a culture of "coerced consent." Benchmarked against OECD privacy principles and GDPR Recitals 40, 50, and 73, the findings indicate that Indonesia's data protection regime remains primarily declarative rather than substantive. The research argues for a strategic shift in the national legal paradigm, moving beyond isolated administrative sanctions toward a synchronization of personal data protection and criminal law. Key recommendations include the urgent operationalization of an independent Personal Data Protection Authority, the formalization of state vicarious liability for public-sector breaches, and the implementation of a reversal of the burden of proof in digital litigation to balance the scales for marginalized data subjects. Ultimately, this study asserts that protecting digital personhood is a prerequisite for dismantling the predatory criminal ecosystems that currently thrive on the unauthorized commodification of personal information.

Keywords:
Personal Data Protection; Online Gambling; Data Commodification

1. Introduction
The protection of personal data is a fundamental human right and a core component of individual privacy. This principle is enshrined in the preamble of the Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (the "PDP Law"). Although the PDP Law serves as a relatively new statutory framework, the concept of personal data protection has been embedded in the Indonesian constitutional landscape since the Second Amendment to the 1945 Constitution. Article 28G Paragraph (1) explicitly stipulates that every individual possesses

the right to the protection of their person (including personal data), family, honor, dignity, and property under their control. Furthermore, every individual is entitled to a sense of security and protection from threats or fear that undermine their freedom to act in accordance with their fundamental rights. Personal data protection is thus a critical aspect of human rights, emphasizing the individual's right to secure and guaranteed personal information. In instances of breach or misuse, data subjects are entitled to clarification and legal recourse. This right to privacy is inherently sensitive, as it involves personal information that is highly susceptible to exploitation.

Rapid technological advancements have fundamentally altered how individuals interact with online services. As a state governed by the rule of law, Indonesia utilizes legal frameworks as the foundation for all aspects of life, including the protection of personal data as an inseparable element of the right to privacy. This protection aims to safeguard the integrity and dignity of every individual as a user of online services. Currently, the burgeoning economic value of personal data has transformed it into a high-value asset or commodity. While the data of a single individual may hold negligible value, the aggregate data of thousands or millions of users constitutes a formidable asset, particularly within the practice of targeted advertising (Martha, 2025). User data—ranging from search history, geolocation, and online behavioral tendencies to financial records and even emotional triggers—is harvested, packaged, and sold to advertisers, app developers, and data brokers. This information is not merely used to enhance user convenience and security; it can also be weaponized within various digital industries (Tameo et al., 2025).

Concerns regarding the exploitation of personal data are no longer merely theoretical. Such speculation is well-founded, particularly when parties with access to massive databases may misuse them for private gain. This necessitates robust accountability mechanisms for personal data protection. Regulation alone is insufficient; implementation must be stringent and accompanied by clear sanctions for misuse. When data collected by the government or private entities can easily fall into the hands of third parties, individuals are not only exposed to privacy violations but also to significant risks such as fraud, identity theft, and other exploitative practices (Anggoro & Santoso, 2025).

This predicament raises a deeper question: if personal data cannot be entrusted to private corporations driven by self-interest, to whom can we turn other than the state? However, public trust in government institutions as the primary custodians of personal data is eroding due to recurrent data breaches within official state systems. One case that has intensified public concern is the May 2025 hacking of the PeduliLindungi system, where the pedulilindungi.id domain—previously managed by the government—was compromised and redirected users to online gambling sites. PeduliLindungi was an application developed by the Ministry of Health in early 2020 to manage the COVID-19 pandemic (Abdullah et al., 2025). The primary motivation for public adoption was its role as the exclusive gateway for vaccination certificates and electronic Health Alert Cards (eHAC) for international travel. Downloading the app and scanning QR codes was mandatory for entering public spaces. In September 2022, it was announced that PeduliLindungi would transition into a broader health application named SatuSehat Mobile, utilizing its existing infrastructure. However, following the revocation of public activity restrictions on January 1, 2023, the Ministry of Health stated that the application was no longer mandatory, leading to a decline in usage (Surbakti, 2025). Despite the transition to SatuSehat and its new domain (satusehat.kemkes.go.id), a significant portion of the Indonesian public continues to associate the PeduliLindungi brand with the government's active digital health program. The official explanation regarding the 2025 hack merely stated that the Ministry was no longer the manager of the old domain. Consequently, many users were unaware the site was defunct, exacerbating public shock when it was discovered the domain was being used to promote online gambling. Social media discourse suggests a widespread fear that the database—containing the personal information of approximately 105 million Indonesians—may have been compromised, leaving it in an exceptionally vulnerable position.

The government has a troubled track record regarding the security of citizen data stored within the PeduliLindungi/SatuSehat ecosystem. In 2021, the data of 1.3 million residents, including the vaccination certificate of former President Joko Widodo, was leaked. In 2022, a hacker known as "Bjorka" distributed approximately 3.2 billion data points belonging to 94 million citizens registered in the system. The leaked data, which included biodata, vaccination records, geolocations, and check-in histories, was sold for US$100,000 in Bitcoin (Surbakti, 2025).

Naturally, public confidence in the government's ability to secure personal data remains low. Despite the enactment of the PDP Law, sentiment indicates that the state is not yet fully trusted to protect its residents' information. On the social media platform X (formerly Twitter), user @bangherwin remarked: "The Pedulilindungi.id site... has now turned into an online gambling site. The state has failed to protect its citizens' data, [again]." This post garnered over

29,000 likes and 13,000 retweets. Another user, @cupang_fish, responded: "Imagine, something as 'trivial' [as PeduliLindungi] can be [twisted] into online gambling. What about something as large as Danantara? Both are [government-managed]" (Imogen, 2025).

A disturbing possibility emerges: what if parties with access to these databases do not merely use them for surveillance or profit, but strategically target vulnerable populations? Research indicates that adolescents and lower socioeconomic groups are most susceptible to the negative impacts of online gambling in Indonesia. These demographics often lack financial literacy and access to psychological support, making them easy targets for manipulative advertising. Conversely, in jurisdictions where gambling is legalized, demographic spread is often more balanced, though international trends show an alarming increase in targeting children through integrated advertising tactics. In Indonesia, because gambling is a social taboo, public literacy regarding its risks remains low. The convergence of algorithmic demographic targeting and societal vulnerability has transformed online gambling from an individual threat into a systemic social crisis.

This situation brings the broader issue of gambling in Indonesia into focus. Although legislation strictly prohibits all forms of gambling, the practice remains pervasive online. Digital platforms are saturated with advertisements for slot sites, lottery (togel), sports betting, and even predatory online lending apps or mobile games featuring loot box mechanics. Furthermore, Indonesian nationals abroad have been found operating online gambling hubs specifically targeting the local Indonesian market. Because gambling is prohibited, the entire industry operates outside the reach of official regulation, bypassing age verification, residency checks, and fraud prevention. Paradoxically, total prohibition has fostered an uncontrolled black market that is far more dangerous than a regulated environment (Fahrudin et al., 2024).

The severity of this crisis is reflected in data from the Financial Transaction Reports and Analysis Center (PPATK), showing a massive turnover of funds. In 2023, transactions related to online gambling reached IDR 327 trillion; in the first quarter of 2024 alone, this figure hit IDR 110 trillion. Most alarmingly, PPATK recorded that 197,540 children aged 11 to 19 were involved in online gambling, with transactions totaling IDR 293.4 billion (Fahrudin et al., 2024). This demonstrates that the illegal online gambling industry is actively exploiting the most vulnerable members of society.

Based on the aforementioned context, this study formulates the following legal problems:

1. What is the legal standing of personal data subjects within the data protection legal system regarding the commodification of personal data?
2. What is the legal protection for personal data subjects against the misuse of personal data for online gambling purposes?

Based on the research problems identified above, the objectives of this study are, first, to analyze and determine the legal standing of personal data subjects within the Indonesian legal framework, specifically addressing the challenges posed by the increasing commodification of personal information in the digital economy. Second, to evaluate the effectiveness of current legal protections and state accountability mechanisms in safeguarding data subjects against the unauthorized exploitation of their personal data for illegal activities, particularly online gambling. Lastly, to provide a critical perspective on the urgency of strengthening the implementation of the PDP Law to restore public trust and mitigate the systemic risks faced by vulnerable demographics in the digital landscape.

2. Method

This study is conducted using a normative legal research method, which prioritizes the analysis of legal norms, statutory frameworks, and doctrinal principles. This methodology is selected to facilitate a rigorous evaluation of the legal synchronization between the PDP Law and the constitutional mandates of the Republic of Indonesia. By situating the law as a structured system of norms, the research aims to pinpoint specific regulatory voids that allow for the commodification and subsequent exploitation of personal data. To provide a comprehensive analysis, the study adopts both a statutory approach and a conceptual approach. While the statutory approach scrutinizes the consistency of domestic regulations, the conceptual approach allows for a deeper exploration of how personal data has evolved from a fundamental human right into a high-value commodity, thereby necessitating a re-evaluation of the data subject's legal standing.

The foundation of this research rests upon a tripartite structure of legal materials. Primary legal materials, which carry binding authority, are central to this analysis. Furthermore, Law Number 27 of 2022 on Personal Data

Protection serves as the core framework, supplemented by the General Data Protection Regulation (Regulation (EU) 2016/679) to provide a global comparative standard. These primary sources are bolstered by secondary legal materials, which provide interpretative depth through academic journals

3. Results and Discussions

3.1 The Legal Standing of Personal Data Subjects and the Crisis of Commodification

3.1.1 Structural Asymmetry and the Rise of Surveillance Capitalism

Violations of personal data protection often stem from a fundamental imbalance in the distribution of information and control. A significant regulatory lag exists where digital innovation outpaces the legal frameworks designed to govern it. Data controllers frequently operate beyond the context understood by data subjects, creating a relational imbalance where individual privacy expectations are no longer aligned with actual data processing practices. The lack of algorithmic transparency further exacerbates this power disparity, rendering automated decision-making processes opaque and beyond the oversight of the data subject (Nedzhvetskaya, 2019). The relationship between the data subject and the controllers/processors is not merely contractual; it reflects a hegemonic power dynamic.

In the modern digital landscape, individuals lack the capacity to influence how their data is utilized. This asymmetry is a prerequisite for data-driven business models, where economic profit and power are concentrated among those with superior technological and analytical resources. Consequently, the data subject loses autonomy over their own personal information (García, 2024). The relationship is inherently asymmetric because controllers and processors possess greater technological infrastructure and information access. Data subjects typically lack adequate knowledge regarding the extent, purpose, and ultimate users of their data. Conversely, data titans such as tech companies, government agencies, or data brokers, possess the technical and legal prowess to harvest, process, and aggregate data on a massive scale. Thus, one party exerts near-total control, while the other maintains marginalized or non-existent control over their own digital identity (Guillou-Landreat et al., 2021).

In this digital ecosystem, personal data is treated as a high-value economic commodity. Data holders profit through behavioral analysis, service personalization, and third-party data sales, while subjects rarely receive direct economic benefits from this exploitation. This reflects a form of structural dominance, where data holders possess superior bargaining power through their control over digital infrastructure. Access to digital services is often predicated on the surrender of personal data, leading to a phenomenon of coerced consent, where subjects are subtly forced to agree to data collection without fully grasping the long-term implications (Nedzhvetskaya, 2019). This inequality is reinforced by informational capitalism, where data is the primary source of power. Controllers not only manage information flows but also shape social, political, and economic behavior through predictive algorithms.

As previously noted, technology companies and social media platforms act as the primary agents transforming human digital activity into a new economic resource. Through this process, personal data becomes the raw material for behavioral prediction algorithms and personalized marketing strategies. Modern society operates within a data-driven economy, described by Shoshana Zuboff as "Surveillance Capitalism." This model centers on the exploitation of human experience as free raw material for translation into behavioral data. According to Zuboff, this system emerged when tech giants discovered that human behavior could be modified, predicted, and sold as behavioral surplus (Zuboff, 2015).

Within this framework, personal data is no longer a passive record but an extractive resource. Every digital interaction is converted into measurable data to fuel the digital economy. It serves as a strategic instrument of power, allowing interested parties to influence the behavior of data subjects through behavioral patterning and the collective shaping of public opinion (Zuboff, 2019). Zuboff further explains that this leads to "instrumentarian power": a form of power that does not oppress through direct force but through subtle, invisible behavioral engineering. Algorithms and advertising systems are used to mold human decisions without the user's knowledge, causing subjects to lose their autonomy as their own data is used to manipulate their preferences (Zuboff, 2015).

Surveillance capitalism marks a shift from a production economy to a prediction economy. Economic value is derived from the ability to predict and direct future human behavior. This involves massive data extraction, including latent data generated without user awareness, such as geolocation, usage duration, and emotional states (Couldry & Mejias, 2018). Consequently, daily human life is commodified, and the power imbalance is no longer based on physical capital but on the ownership of data and algorithms (Nadler & McGuigan, 2018). Legal protection,

therefore, must be viewed not merely as an administrative task but as a broader struggle to defend individual freedom and democracy in the digital age.

The theory of surveillance capitalism provides a foundation for understanding how the online gambling industry exploits personal data. Online gambling marketing relies heavily on behavioral surplus to predict an individual's emotional and psychological tendencies. Using advanced advertising kits integrated into platforms like Google, YouTube, Meta, and TikTok, these industries can precisely target individuals deemed vulnerable to impulsive behavior, such as those exhibiting patterns of stress, loneliness, or a need for social validation (Rossi & Nairn, 2022).

Research indicates that the most vulnerable groups—adolescents and those from lower socioeconomic backgrounds—are often targeted through a combination of demographic factors and pre-existing psychological conditions. Young adults (18–25) exhibit higher rates of "problem gambling" as they transition to financial independence (Nadler & McGuigan, 2018). Similarly, individuals facing financial pressure are more susceptible to "quick-win" promises. This vulnerability is amplified by predatory digital marketing, where gambling ads are camouflaged as regular content, such as free bet offers (Torrance et al., 2021).

Personal data collected from various sources, including financial apps and illegal data brokers, is used to build high-precision behavioral prediction models. These models identify exactly when a person is in an emotional state most ripe for exploitation. This reflects a phase of surveillance capitalism where the digital economy depends on the manipulation of emotional states as a profit instrument (Galmés-Cerezo et al., 2025). Thus, the legal protection of data subjects in the context of online gambling is inextricably linked to a critique of the logic of surveillance capitalism itself.

3.1.2 Navigating the Indonesian Legal Landscape: Prospects and Barriers

If such abuses occur in Indonesia, they can be addressed through the PDP Law supplemented by the ITE Law: Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. Technically, the Indonesian framework establishes a strong foundation by positioning individuals as the primary owners of their data, requiring consent, transparency, and legitimate purpose. However, practical implementation remains stymied by several factors:

1. Inoperative PDP Authority: The yet-to-be-established Personal Data Protection Authority (Lembaga PDP) creates an institutional vacuum. Without this independent body, there is no centralized regulator to conduct audits, impose administrative fines, or provide technical guidelines for data security (Solikhah, 2025).
2. Weak Law Enforcement Capacity: Law enforcement agencies often lack the digital forensic expertise required to trace data leaks or verify illegal commodification. Cross-agency coordination remains ad hoc, leading to slow responses to breaches (Taufiq & Kenyo, 2025).
3. Barriers to Civil Litigation: While the PDP Law allows for compensation claims (Article 12), the probability of success is low due to a lack of jurisprudence and clear standards for proving immaterial loss (e.g., anxiety or loss of control) (Budiman, 2023).
4. Criminal Recourse: Filing criminal reports under Articles 65 and 67 of the PDP Law or Article 27(2) of the ITE Law is technically "sharper" and easier to prove, as the focus is on the perpetrator's actions rather than the victim's loss. However, jurisdictional limitations pose a major challenge, as data brokers often operate anonymously from overseas (Ngompat & Maran, 2024).
5. Lack of Recovery Infrastructure: Unlike the EU's GDPR, Indonesia lacks a national data breach register, a transparency portal, or "privacy dashboards." This places the administrative burden entirely on the individual data subject to manually contact companies and request data deletion, often without a guarantee of compliance (Taufiq & Kenyo, 2025).

Having this said, while the legal standing of the data subject is theoretically robust under Indonesian law, the reality is a landscape of procedural hurdles and institutional unreadiness that leaves citizens highly vulnerable to the predatory cycles of the global data-driven economy.

The PDP Law provides several critical avenues for the data subject to regain agency. However, their effectiveness is heavily contingent on secondary regulations that have yet to be fully realized. The Principle of Purpose and Limitation (Articles 27 & 29): The PDP Law mandates that data processing must have a specific, limited purpose. When a data controller—such as a government health app or a private service—collects data for one reason (e.g.,

pandemic monitoring) but allows it to be leaked or diverted to another (e.g., gambling site redirects), it constitutes a severe violation of Article 27 Paragraph (2) of the ITE Law in conjunction with the PDP Law's purpose limitation.
Moreover, the Right to Compensation (Article 12): This article is the primary legal basis of the law for individuals. It allows subjects to sue for both material and immaterial damages. However, in the context of online gambling, the damage is often psychological or social, which Indonesian courts find notoriously difficult to quantify without standardized damages assessment guidelines. Meanhile, Administrative Sanctions (Article 57): The law threatens massive fines (up to 2% of annual revenue). Yet, without an active Data Protection Authority, these sanctions remain a "paper tiger." The lack of an independent regulator means there is no "referee" to verify if a company's security breach was a result of gross negligence or a sophisticated state-sponsored hack.

3.1.3 Global Lessons and the Enforcement Deficit

While large-scale documented cases in Indonesia are still emerging, international precedents demonstrate the severe risks:
1. Meta and UK Gambling Sites: Reports revealed that UK gambling companies secretly tracked visitors using the "Meta Pixel" and transferred data to Meta without consent. Users were subsequently bombarded with gambling ads across social media, targeting even those struggling with addiction (Torrance et al., 2021).
2. Uber's GDPR Violation: In August 2024, Dutch regulators fined Uber €290 million for failing to protect European drivers' data during international transfers to the US, highlighting the risks of sensitive data (location, medical, and criminal records) being processed without extra protections (Fisher et al., 2025).
3. Facebook's Emotional Targeting: In 2017, leaked documents showed Facebook offered advertisers the ability to target 6.4 million users—including minors as young as 14—when they were in vulnerable psychological states (e.g., feeling "worthless" or "anxious") (Montgomery, 2015).
Even with the best laws, the technical reality of the digital economy creates an enforcement deficit. When personal data is commodified for online gambling, it often travels through a complex shadow supply chain involving illegal data brokers and offshore servers. First, Forensic Limitations: Indonesian law enforcement currently faces a steep learning curve in digital chain-of-custody. Proving that "Data Leak A" led directly to "Gambling Ad B" requires a level of forensic tracing that is currently rare in domestic litigation (Rossi & Nairn, 2024). Second, the Anonymity of Data Brokers: While the PDP Law punishes the "use" of data not belonging to oneself (Article 65), the perpetrators are often anonymous entities on the dark web. This makes the criminal path—though theoretically sharper—practically difficult unless the state invests heavily in international cyber-cooperation and Interpol-level data tracking (Tran et al., 2024).
The legal standing of the personal data subject in Indonesia currently exists in a state of normative paradox. On one hand, the PDP Law provides a robust, human-rights-centric framework that mirrors the high standards of the GDPR, granting individuals the right to be protected from the predatory cycles of Surveillance Capitalism. On the other hand, the practical infrastructure of protection is marred by institutional unreadiness and the absence of a central enforcement authority.
The commodification of data for online gambling is not merely a technical breach; it is a manifestation of instrumentarian power that exploits the most vulnerable demographics of society. Until the Personal Data Protection Authority is fully operational and the courts establish clear precedents for immaterial losses, the data subject remains a "product" rather than a "citizen" in the digital marketplace. The transition from a production economy to a prediction economy requires more than just statutes—it requires a state-led commitment to dismantling the asymmetry of power that currently favors the exploiters over the exploited.

3.2 Legal Foundations for Protecting Data Subjects in Online Gambling

3.2.1 Assessing Legal Efficacy: Theoretical and Comparative Benchmarks

In assessing the efficacy of legal protections for Personal Data Subjects whose information is exploited for online gambling, Soerjono Soekanto's theory of legal effectiveness provides a critically relevant analytical framework. Soekanto asserts that the success of a law does not rest solely on the normative quality of its statutes, but on the synergy of five primary factors: (1) the law itself, (2) law enforcement, (3) facilities or infrastructure, (4) the community, and (5) cultural factors (Supeno et al., 2025). These elements operate simultaneously to determine

whether a rule functions effectively in practice. Applying this theory allows us to map systemic gaps that facilitate recurring data misuse.

1. The Statutory Factor: Normatively, Indonesia has established a foundation through the PDP Law, which prohibits illegal processing and grants fundamental rights such as access, objection, and compensation. However, this framework is not yet fully operational. The absence of comprehensive technical regulations means implementation is often more declarative than substantive. Furthermore, the lack of a robust verification system for processing purposes makes purpose limitation difficult to monitor, allowing data to migrate unlawfully into online gambling ecosystems (Lihawa, 2025). The regulatory vacuum regarding data brokers remains a critical vulnerability, as these actors often serve as the primary conduits for data leaks used in illicit gambling registrations.
2. The Law Enforcement Factor: In practice, enforcement involves a fragmented array of actors, including the National Police, the Ministry of Communication and Digital Affairs, PPATK, and the OJK. This fragmentation is exacerbated by the delayed formation of a centralized data protection authority. Digital forensic capacity in Indonesia remains limited, particularly when data flows involve offshore brokers (Simbolon & Juwono, 2022). Consequently, enforcement efforts are frequently directed toward the act of gambling itself (the symptom) rather than the personal data violation (the cause), despite these being distinct offenses that require independent adjudication.
3. The Facilities Factor: Technical limitations hinder effective protection. Indonesia lacks a national data breach register to serve as a transparency and early-warning system. Furthermore, there is no centralized consumer dashboard, similar to those mandated by the EU GDPR, which would grant data subjects greater control (Haditama & Sugianto, 2025). Without centralized complaint channels or mandatory national security standards, the movement of data through the black market remains untraceable, rendering the rights of the data subject unenforceable in reality.
4. The Community Factor: Public awareness regarding data risks remains notably low. This is characterized by the habitual sharing of sensitive identifiers, such as ID cards, via insecure platforms. In the context of online gambling, many individuals are unaware that their data can be commodified for account verification or illicit financial routing (Kuasa & Jaya, 2022). This normalization of careless data sharing creates a structural vulnerability, rendering the rights provided by the PDP Law ineffective because the community lacks the awareness to exercise them.
5. The Cultural Factor: Legal effectiveness is heavily influenced by public trust in enforcement agencies. Many victims of data breaches choose not to report incidents, fearing a lack of follow-up or a convoluted bureaucracy. This culture of underreporting creates a cycle of impunity and weakens the state's ability to identify criminal networks (Azhari, 2024). Furthermore, a segment of society still perceives online gambling as harmless entertainment. This permissive culture creates a fertile market for stolen data; as long as the demand for illegal services remains high and the risks are underestimated, legal protections will continue to lag.

An assessment of the current landscape against the OECD Guidelines reveals several fundamental failures in protection:

1. Collection Limitation Principle: This principle emphasizes lawful data collection and informed consent. In the gambling industry, data is frequently harvested without a legal basis through phishing or scraping. Existing regulations are currently insufficient to curb massive, uncontrolled collection by offshore actors.
2. Data Quality Principle: Many Indonesian institutions lack mechanisms to ensure data remains accurate and relevant. Poorly managed or unverified data creates a landscape where misinformation is easily exploited.
3. Purpose Specification & Use Limitation: While data may be initially collected for legitimate ends (e.g., e-commerce or fintech), it is often traded or leaked to illegal entities. Once data falls into unauthorized hands, there are no guarantees it will not be used for purposes entirely unrelated to the original consent.
4. Security Safeguards Principle: Recurring leaks highlight a severe weakness in domestic security standards. The absence of strict administrative sanctions for negligence exacerbates this vulnerability.
5. Openness & Participation Principles: Post-breach transparency is severely lacking. Victims are rarely informed about how their data was misused or who is accountable. Because remediation pathways remain obscure, the individual participation of data subjects is effectively marginalized.
6. Accountability Principle: Accountability mechanisms have not yet matured. It remains unclear who bears ultimate responsibility for leaks or how the state can effectively penalize controllers who fail to safeguard data (Azhari, 2024).

The following GDPR recitals provide a comparative benchmark for the deficiencies in the Indonesian system:

1. Recital 40 (Lawfulness of Processing): This recital mandates that processing must have a clear, specific, and provable legal basis. In Indonesia, while the PDP Law outlines such bases, there is no robust mechanism to ensure validity. Controllers are not required to maintain the detailed documentation seen in the GDPR, making the legal basis often anecdotal and unverifiable. In the case of online gambling, data diverted for illegal acts lacks any legal standing, yet no regulatory trigger automatically classifies this as unlawful processing.
2. Recital 50 (Compatible Use): This principle asserts that data should only be used for purposes compatible with the original collection. Changes in purpose require a compatibility assessment—evaluating the context of collection and the risks to the subject. While the PDP Law mentions purpose limitation, it does not mandate a documented assessment. Consequently, data collected for public or commercial services is easily transitioned into incompatible uses, such as illegal gambling offers or identity fraud, without a formal legal breach being recognized in real-time.
3. Recital 73 (Restrictions and Public Interest): This recital emphasizes that data protection must persist even in matters of public security. Comparing this to Indonesia, protection for victims remains sub-optimal. While the state has a mandate to eradicate illegal gambling, the legal framework has not yet explicitly formalized the causal link between personal data misuse and subsequent criminal activity. When processing is diverted for unlawful purposes, the entire chain of processing should lose its legal legitimacy (Pickering & Blaszczynski, 2021); however, the Indonesian infrastructure is not yet equipped to adjudicate this comprehensively.

3.2.2 Reconstructing Accountability: From State Liability to the Burden of Proof

The hacking of the PeduliLindungi (now SatuSehat) system presents a unique legal challenge regarding the vicarious liability of the state as a public data controller. In the Indonesian legal context, when the state mandates the use of an application as a prerequisite for exercising basic civil liberties—such as freedom of movement during a pandemic—the relationship between the state and the citizen ceases to be a mere service-provision dynamic and becomes one of compulsory entrustment. Consequently, the state's failure to secure the SatuSehat database, which subsequently led to the redirection of users to gambling domains, cannot be dismissed as a third-party criminal act alone. Under the principle of Onrechtmatige Overheidsdaad (Unlawful Act by the Government), the state holds a heightened duty of care (Iqbal et al., 2025). The legal argument here is that the state, through the Ministry of Health, serves as the ultimate custodian of the national digital health identity. When this infrastructure is compromised due to inadequate maintenance of defunct domains or weak backend security, the state becomes negligent by omission, making it liable for the resultant social harm, including the exposure of citizens to predatory gambling networks.

The legitimacy of data processing for online gambling often relies on the existence of prior consent, yet in the Indonesian digital ecosystem, this consent is frequently legally fragile. Applying GDPR Recital 43 as an analytical benchmark, it is evident that consent cannot be considered freely given if there is a significant power imbalance between the data subject and the controller. In the case of government-mandated apps, citizens were essentially "coerced" into data submission; refusing to use the app meant a forfeiture of the right to enter public spaces or travel. This coerced consent creates a downstream legal nullity (Sexton et al., 2018). If the initial collection was predicated on a power imbalance, any secondary use of that data—whether through leakage or illicit sale to gambling operators—lacks a valid legal root. This suggests that the PDP Law must be interpreted strictly: when the state or a dominant platform forces data submission, the standard for "compatible use" must be near-absolute, and any deviation should automatically trigger strict liability for the controller.

One of the most significant barriers to achieving justice for data subjects is the technical difficulty of establishing a causal link between a specific leak and the subsequent receipt of gambling-related solicitations (Rott, 2025). Under current Indonesian procedural law, the burden of proof rests on the plaintiff (the victim), who is ill-equipped to perform the digital forensics required to trace data provenance across the dark web. To resolve this, this research proposes a normative shift toward the Reversal of the Burden of Proof (the doctrine of Res Ipsa Loquitur in data litigation). Under this model, if a data subject can demonstrate a temporal correlation—for instance, receiving targeted gambling ads shortly after a documented breach of a specific controller—the law should maintain a presumptive negligence on the part of that controller. The burden would then shift to the corporation or government agency to prove that their security protocols were not only compliant with the PDP Law but were also not the source of the specific leak. This shift is essential to balance the scales of justice in an era of informational capitalism.

3.2.3 Strengthening the Framework: Institutional Independence and Legal Synchronization

Finally, the transition from a paper tiger framework to an active defense system depends entirely on the institutional design of the Personal Data Protection Authority. This research argues that for the authority to be effective, it must avoid the pitfalls of being a sub-department within a ministry, which would create a conflict of interest when investigating state-sponsored breaches. Instead, Indonesia should adopt an independent regulatory model, reporting directly to the President or Parliament, similar to the status of the KPK or the Ombudsman. This authority must be granted the power to not only impose administrative fines but also to issue binding technical mandates and conduct unannounced audits on both private and public data controllers. By comparing the Indonesian situation with the UK's Information Commissioner's Office (ICO), it is clear that only a body with both political independence and high-level digital forensic capabilities can effectively dismantle the illegal data-brokering networks that currently sustain the online gambling industry.

The ideal model for data protection and the mitigation of digital crime necessitates a comprehensive synchronization between the personal data protection regime and the criminal justice system. It is imperative that these two legal spheres do not operate in isolation, overlap inefficiently, or remain in a state of mutual dependency (Ruiyin, 2025). This synchronization serves as a conceptual framework that explicitly bridges the gap between the domain of data misuse (civil/administrative matters) and the domain of criminality (criminal matters). In the context of data misuse for online gambling as well as other related illicit activities such as online fraud, predatory lending, phishing, and digital extortion, this integration is vital. It clarifies that data-driven crimes cannot be perceived merely as privacy violations; rather, they must be understood as criminal resources that enable and fortify a wider ecosystem of illegal activity (Dresch & Faleiros Júnior, 2025).

Legal synchronization is required to establish a clear nexus between personal data privacy breaches and the various forms of modern crime that exploit them. In many instances, data leaks act as the primary catalyst for these crimes; however, the Indonesian legal system frequently continues to treat data violations as isolated administrative issues, detached from the downstream criminal acts they facilitate. Consequently, a normative bridge is needed to harmonize the personal data protection regime with the criminal and sectoral legal frameworks, including the Criminal Code and the ITE Law. Such harmony ensures that the legal process can track the entire trajectory of the crime. A pivotal element of this synchronization is the formalization of a causal link between the act of data misuse and the subsequent crimes that arise from it. With a robust framework in place, law enforcement can determine that a data controller's failure to exercise due diligenceresulting in a leak exploited for fraud or illegal gambling is not merely an administrative lapse, but a statutory aggravating factor in criminal proceedings. This approach strengthens accountability and ensures that data protection serves as an integral component of the national strategy to combat digital crime.

Strengthening prevention and deterrence must begin with a paradigm shift, moving from a reactive approach—which only triggers after a violation has occurred—to a proactive one that prevents breaches during the collection and processing stages. In an increasingly complex digital ecosystem, the point of vulnerability is situated at the upstream level, where data is gathered, processed, and distributed without adequate security mechanisms. Effective protection requires the implementation of deterrent sanctions that are both firm and intimidating. Sanctions must be applied proportionately yet severely enough to ensure that negligence or non-compliance is not dismissed as a mere cost of doing business by corporations.

In cases involving willful blindness or direct involvement in channeling data toward illegal activities—such as controllers or processors who are aware of unauthorized access but fail to initiate mitigation—heightened penalties should be imposed. This approach compels all stakeholders to recognize that negligence or omission does not only compromise the integrity of the data system and harm thousands of victims but also fundamentally undermines their own legal interests. By combining proactive prevention with stringent sanctions, the legal system can construct multi-layered barriers that stop data leaks at their source while reaffirming that any misuse will result in significant legal consequences.

Equally important, the establishment of the Personal Data Protection Authority and the formalization of governmental responses are foundational to building a truly effective protection system. The current institutional structure remains insufficient in handling data violations with the necessary speed, coordination, and consistency, particularly when breaches are linked to complex crimes like online gambling, digital fraud, or cross-platform financial exploitation. Therefore, a comprehensive restructuring is required so that enforcement, investigation,

oversight, and the imposition of sanctions are no longer fragmented across various ministries and agencies. A core step is the formation of an independent Personal Data Protection Authority with clear authority, as mandated by the PDP Law. This ensures that victims have a transparent channel for reporting, while the state can respond to incidents swiftly through standardized procedures.

4. Conclusion

The convergence of rapid digitalization and the burgeoning data-driven economy has transformed personal information from a private attribute into a high-value global commodity. However, as this research has demonstrated, the transition from a production-based economy to a prediction economy, driven by the logic of surveillance capitalism, has created a profound asymmetry of power between individual data subjects and the institutional controllers who harvest their information. In the Indonesian context, this imbalance is most visible in the systemic exploitation of personal data to fuel the illegal online gambling industry. This phenomenon is not merely a technical failure or an administrative lapse, it is a fundamental violation of digital personhood that disproportionately targets the most vulnerable demographics of society.

Through the analytical lens of Soerjono Soekanto's legal effectiveness theory, it is evident that the current protection of personal data in Indonesia remains largely nominal rather than substantive. While the enactment of the PDP Law provided a long-awaited normative foundation, the framework is currently hindered by institutional inertia and the absence of a fully operational, independent Data Protection Authority. This regulatory vacuum, combined with a fragmented law enforcement landscape and a social culture of digital nonchalance, has allowed personal data to become a primary criminal resource. Benchmarking these deficiencies against the global standards of the OECD and the GDPR highlights a critical need for Indonesia to formalize the causal link between upstream data negligence and downstream digital criminality.

To restore the autonomy of the data subject and mitigate the social harm caused by online gambling, Indonesia must move toward a model of legal synchronization. This requires a paradigm shift from reactive enforcement to proactive deterrence, where the failure to secure data is recognized as an integral facilitator of crime. The legal system must bridge the gap between administrative privacy standards and criminal accountability, ensuring that sanctions are sufficiently severe to deter corporate negligence. Ultimately, the protection of personal data must be treated as a cornerstone of national security and human dignity. Only by establishing a centralized, independent oversight body and fostering a society that values digital rights can Indonesia effectively dismantle the extractive ecosystems that currently exploit its citizens' private lives for illicit profit.

Acknowledgments

The blessed completion of this writing would have been impossible without the support and assistance of various parties, especially the faculty members of faculty of law Universitas Pelita Harapan (all in Main Campus, Medan Campus and Surabaya Campus), all the partners and staffs of Seiwa Ginza Law Office for providing meaningful information, data, and in-depth understanding toward the upcoming legal issues related to online gambling and PDP specifically.

References

Abdullah, M., Lismiati, I., & Sapsudin, A. (2025). The Task of Legal Protection for Indonesian Citizens from Online Gambling Exploitation in the Perspective of Law Enforcement in the Digital Era. Journal of Law, Politic and Humanities, 5(5 SE-Articles), 3876–3886. https://doi.org/10.38035/jlph.v5i5.1947

Anggoro, T. C., & Santoso, B. (2025). Prevention of online gambling crimes to maintain social structure stability. Priviet Social Sciences Journal, 5(9 SE-Articles), 66–78. https://doi.org/10.55942/pssj.v5i9.654

Azhari, Y. (2024). Optimization of Legal Support for State Defense and Security Interests in Indonesia. Pena Justisia: Media Komunikasi Dan Kajian Hukum, 23(3), 1777–1796. https://doi.org/10.31941/pj.v23i3.5556

Budiman, R. (2023). The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022. Jurnal Smart Hukum (JSH), 2(1 SE-Articles), 24–36. https://doi.org/10.55299/jsh.v2i1.1352

Couldry, N., & Mejias, U. A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. Television & New Media, 20(4), 336–349. https://doi.org/10.1177/1527476418796632

Dresch, R. de F. V., & Faleiros Júnior, J. L. de M. (2025). Special strict civil liability in Brazil's General Data Protection Law. Brazilian Journal of Law, Technology and Innovation, 2(2 SE-Articles), 98–128. https://doi.org/10.59224/bjlti.v2i2.98-128

Fahrudin, A., Satispi, E., Subardhini, M., Andayani, R. H. R., Jayaputra, A., Yuniarti, L., Wijayanti, F., & Suryani, S. (2024). Online gambling addiction: Problems and solutions for policymakers and stakeholders in Indonesia. Journal of Infrastructure, Policy and Development, 8(11), 1–17. https://doi.org/10.24294/jipd.v8i11.9077

Fisher, M. L., Piper, T., Fitzpatrick, M., Mavi, S., Retzer, A., Bradbury-Jones, C., Montgomery, P., Melendez-Torres, G. J., Kirby, J., Chandan, J. S., & Bedford, K. (2025). Legal and regulatory responses to online gambling harms: a scoping review of evidence. Harm Reduction Journal, 22(1), 163. https://doi.org/10.1186/s12954-025-01292-y

Galmés-Cerezo, M., López-Aza, C., & Gema Martinez-Navarro. (2025). Responsible Marketing Communication in Online Gambling: A Systematic Review of Strategies Targeting Youth. Review of Communication Research, 13, 189–208. https://doi.org/10.52152/rcr.v13.13

García, C. S. (2024). Digital expansionism and big tech companies: consequences in democracies of the European Union. Humanities and Social Sciences Communications, 11(1), 448. https://doi.org/10.1057/s41599-024-02924-7

Guillou-Landreat, M., Gallopel-Morvan, K., Lever, D., Le Goff, D., & Le Reste, J.-Y. (2021). Gambling Marketing Strategies and the Internet: What Do We Know? A Systematic Review. Frontiers in Psychiatry, Volume 12. https://doi.org/10.3389/fpsyt.2021.583817

Haditama, T. K., & Sugianto, F. (2025). A Comparative Analysis of Corporate Criminal Liability for AI-Based Malware: A Study of Indonesian and European Union Law. Indonesia Law Reform Journal, 5(2 SE-Articles), 308–322. https://doi.org/10.22219/ilrej.v5i2.39901

Imogen, L. (2025). Legal Efforts in Tackling the Spread of Online Gambling Promotions on Social Media in Indonesia. International Journal of Multidisciplinary Research and Analysis, 08(03), 1374–1381. https://doi.org/10.47191/ijmra/v8-i03-55

Iqbal, H. M., Hermawan, S., & Nugroho, A. (2025). Bentuk Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional Berdasarkan Hukum Administrasi Negara. Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara, 3(2 SE-Articles), 72–83. https://doi.org/10.55606/eksekusi.v3i2.1825

Kuasa, D. A., & Jaya, F. (2022). Online Gambling Phenomenon: Law & Society. Widya Yuridika: Jurnal Hukum, 5(2 SE-Articles), 345 â€“ 362. https://doi.org/10.31328/wy.v5i2.3572

Lihawa, R. (2025). Digital Privacy Crisis: Legal Protection of Social Media Users' Data in Indonesia's 2022 Law. Estudiante Law Journal, 7(1), 280–296. https://doi.org/10.33756/eslaj.v7i1.30980

Martha, P. A. N. (2025). Legal Review of Online Gambling Crimes in Indonesia and its Impact on the Younger Generation. Journal of Social Research, 4(9), 2213–2218. https://doi.org/10.55324/josr.v4i8.2722

Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. Telecommunications Policy, 39(9), 771–786. https://doi.org/10.1016/j.telpol.2014.12.006

Nadler, A., & McGuigan, L. (2018). An impulse to exploit: the behavioral turn in data-driven marketing. Critical Studies in Media Communication, 35(2), 151–165. https://doi.org/10.1080/15295036.2017.1387279

Nedzhvetskaya, N. (2019). Brave New (Digital) World: Translating Knowledge into Collective Action - Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York, Public Affairs, 2019). European Journal of Sociology, 60(3), 528–533. https://doi.org/10.1017/S0003975619000444

Ngompat, Y. L., & Maran, M. G. M. (2024). Legal Development and Urgency of Personal Data Protection in Indonesia. JILPR Journal Indonesia Law and Policy Review, 5(3 SE-Articles), 627–635. https://doi.org/10.56371/jirpl.v5i3.284

Pickering, D., & Blaszczynski, A. (2021). Paid online convenience samples in gambling studies: questionable data quality. International Gambling Studies, 21(3), 516–536. https://doi.org/10.1080/14459795.2021.1884735

Rossi, R., & Nairn, A. (2022). New Developments in Gambling Marketing: the Rise of Social Media Ads and Its Effect on Youth. Current Addiction Reports, 9(4), 385–391. https://doi.org/10.1007/s40429-022-00457-0

Rossi, R., & Nairn, A. (2024). Navigating the digital age: The need for online-specific gambling marketing regulations. Addiction, 119(9), 1659–1660. https://doi.org/10.1111/add.16578

Rott, P. (2025). Digital Fairness and the Burden of Proof. Journal of Consumer Policy, 48(3), 297–314. https://doi.org/10.1007/s10603-025-09583-4

Ruiyin, L. (2025). Research on the Legal System of Crime of Infringing Citizens' Personal Information. Open Journal of Legal Science, 13(3), 1–8. https://doi.org/10.12677/ojls.2025.133075

Sexton, A., Shepherd, E., Duke-Williams, O., & Eveleigh, A. (2018). The role and nature of consent in government administrative data. Big Data & Society, 5(2), 2053951718819560. https://doi.org/10.1177/2053951718819560

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. Publik (Jurnal Ilmu Administrasi), 11(2), 178–190. https://doi.org/10.31314/pjia.11.2.178-190.2022

Solikhah, M. (2025). Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework. Indonesian Cyber Law Review, 2(1), 1–11. https://doi.org/10.59261/iclr.v2i1.15

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. Journal of Law and Legal Reform, 6(3 SE-Articles), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Surbakti, F. P. S. (2025). Talking with legislators: Educating the public on the dangers of online gambling. Community Empowerment, 10(4), 1040–1048. https://doi.org/10.31603/ce.13285

Tameo, V. E., Tinambunan, M. H., & Rorimpandey, G. C. (2025). Predictive Classification of Online Gambling Impacts in North Sulawesi Using Naive Bayes: Klasifikasi Prediktif Dampak Judi Online di Sulawesi Utara Menggunakan Naive Bayes. Indonesian Journal of Innovation Studies, 26(4), 10–21070. https://doi.org//10.21070/ijins.v26i4.1728

Taufiq, M., & Kenyo, A. S. (2025). The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR. International Journal of Business, Law, and Education, 6(2), 1260–1268. https://doi.org/10.56442/ijble.v6i2.1178

Torrance, J., John, B., Greville, J., O'Hanrahan, M., Davies, N., & Roderique-Davies, G. (2021). Emergent gambling advertising; a rapid review of marketing content, delivery and structural features. BMC Public Health, 21(1), 718. https://doi.org/10.1186/s12889-021-10805-w

Tran, L. T., Wardle, H., Colledge-Frisby, S., Taylor, S., Lynch, M., Rehm, J., Volberg, R., Marionneau, V., Saxena, S., Bunn, C., Farrell, M., & Degenhardt, L. (2024). The prevalence of gambling and problematic gambling: a systematic review and meta-analysis. The Lancet Public Health, 9(8), e594–e613. https://doi.org/10.1016/S2468-2667(24)00126-9

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. In PublicAffairs, New York. PublicAffairs.