International Proceeding
Universitas Tulungagung
2025

CONSUMER PROTECTION IN DIGITAL PAYMENT TRANSACTIONS AND FINTECH CREDIT: RISK ANALYSIS AND REGULATION

Reginaldo Christian[1], Ardian Az Zam Zami[2], Nisda Finda[3], Sulistyo Mahmud[4],Retno Sari Dewi[5]

[1,2,3,4,5] Universitas Tulungagung, Indonesia
[*]reginaldochristian13@gmail.com, sarie.soegito@gmail.com

Abstract

Digital payment systems and fintech lending services in Indonesia have made shopping and borrowing easier, but they also bring new legal and security risks. This article examines the effectiveness of consumer protection regulations governing digital payments and fintech lending in Indonesia using a normative legal approach. The research examines whether existing regulations such as the Consumer Protection Law, Bank Indonesia regulations on payment systems, and the Financial Services Authority (OJK) regulations on consumer protection in the financial sector are sufficient to address issues such as transparent fees, fair debt collection practices, misuse of personal data, and online transaction security. By examining relevant laws, policies, and principles,

this study identified gaps in current regulations and examined how well consumer rights are protected in practice. The results show that while regulations have improved, their implementation remains inconsistent, particularly regarding unauthorized data use and aggressive data collection practices. The study recommends a more integrated, consumer-rights-based approach, with a focus on harmonizing regulations, improving oversight, and establishing clear accountability standards for fintech providers and digital payment platforms.

Keywords: *Consumer Protection, Digital Payments, Fintech Lending, Regulatory Framework, OJK Regulation.*

INTRODUCTION

The rapid growth of digital payment systems and fintech lending services has radically changed the way Indonesians conduct transactions. Platforms like e-wallets, Buy Now Pay Later (BNPL) services, and peer-to-peer (P2P) lending have made financial access easier and more convenient than ever before. However, these developments have also left consumers vulnerable to legal and systemic issues, such as unclear fees, abusive and unlawful debt collection practices, misuse of personal data, and a growing risk of fraud and illegal transactions (Rahardjo, 2022; OJK, 2023). Therefore, it is crucial for us to re-examine whether existing legal regulations in Indonesia such as the Consumer Protection Law (Law No. 8 of 1999), Bank Indonesia regulations on payment systems, and OJK regulations sufficiently provide effective protection for consumers in this ever-evolving digital world. Despite the recent development of new regulations, there remains a significant gap between officially

guaranteed consumer rights and their implementation in practice. For example, cases of unauthorized use of consumer data, misleading information about loan costs, and frightening illegal debt collection practices remain common. This demonstrates the lack of regulatory oversight and compliance among fintech providers (Adrianto, 2023). This persistent problem clearly requires a comprehensive legal analysis to re-examine the consumer protection system in Indonesia, particularly in the digital financial sector.

This research has three objectives. First, to examine the adequacy of consumer protection regulations in Indonesia that govern digital payment platforms and fintech credit services. Second, to identify regulatory gaps or structures that make it difficult to fulfill consumer rights in practice. Third, to provide recommendations to strengthen the legal and regulatory systems governing digital consumer transactions. The method used is normative juridical, focusing on statutory analysis, regulatory interpretation, and doctrinal review of consumer protection principles. Theoretically, this research contributes to the development of consumer protection legal doctrine, particularly as it relates to digital finance and its normative law. By combining legal theory with current regulatory challenges, this research helps improve understanding of digital consumer rights and responsibilities in the fintech sector. From a practical perspective, the results of this research can provide insights for regulators, fintech operators, and policymakers to improve transparency, oversight, and accountability standards for digital financial services.

The novelty of this research lies in its clear focus on how to create a harmonious, rights-based digital financial regulatory framework, a topic that has not been fully addressed in Indonesian legal studies to date. Compared with previous research that focused primarily on consumer complaints or regulations within a single sector, this study provides a more comprehensive and comprehensive evaluation. It combines analysis of laws with cross-sectoral regulations, such as data protection regulations, financial services regulations, and digital transaction protection.(Windani Sri, 2024) The study also introduces a clear responsibility model for fintech providers and digital payment platforms, addressing the academic gap regarding the shared responsibilities of intermediaries and service operators. The analysis reveals that although Indonesia has made significant progress in regulations to protect consumers in digital financial services, their implementation remains inconsistent. Particular problems relate to illegal and non-compliant data collection practices. This study concludes that Indonesia needs a more integrated, transparent, and consumer-focused regulatory approach to ensure clearer laws and greater consumer trust. Several practical recommendations include harmonization of regulations between institutions, strengthening oversight by the Financial Services Authority (OJK) and Bank Indonesia, and implementing clearer standards for information disclosure, risk mitigation, and data governance.

LITERATURE REVIEW

The development of digital payment systems has changed the way people make transactions daily. These systems make transactions faster and more convenient, but also introduce new risks. According to Raghavan (2019), there are key risks such as data misuse, identity theft, transaction errors, and weak security in services like digital wallets and QR code-

based payments. These risks arise because many parties are involved in the digital payment ecosystem, including service providers, payment gateways, and third parties managing the data.

Research by Marbán and Muliro (2022) points out that developing countries face higher risks due to weak digital security infrastructure and low consumer literacy. Meanwhile, the study by Lwin, Pham, and Lee (2020) shows that consumer trust in digital payments is largely determined by three factors: privacy assurance, system security, and transparency in data usage.

In Indonesia, Kurniawati (2022) found that Bank Indonesia, through Regulation PBI 19/12/2017, requires financial technology providers to implement consumer consent principles, protect personal data, maintain system security standards, and provide dispute resolution mechanisms. However, the study also shows that the implementation is still not optimal, especially regarding consumer education and supervision of third parties managing the data.

Fintech lending services provide a technology-based credit system with fast processing, but this also poses significant risks to consumers. Research by Ramakrishnan and Bhat (2021) highlights the risk of over-indebtedness caused by opaque credit scoring algorithms. Meanwhile, Wójcik and MacDonald (2020) conclude that peer-to-peer lending platforms are vulnerable to operational failures and default risks, which can negatively impact the funders.

In the Indonesian context, the study by Handayani and Yuwono (2021) found that many users of credit fintech experience issues such as unethical debt collection, misuse of personal data, and predatory lending practices. This is further supported by Nugroho's (2021) research, which shows that consumer complaints about fintech lending are mostly about misuse of contact data, low cost transparency, intimidating collection practices, and layered interest charges.

Research published in Blantika Multidisciplinary Journal (2025) shows that fintech platforms have a legal responsibility to reduce the risks of fraud and cybercrime. They are required to provide consumer complaint mechanisms and ensure data security in accordance with POJK 13/2018 regulations. The study also highlights that the increasing frequency of phishing, data theft, and fund transfer crimes calls for stronger regulatory responses from both regulators and fintech platforms.

Previous studies by Widiastuti & Santoso (2021) and Suryanto & Wibowo (2022) also highlight that cybersecurity compliance is a major issue in the fintech industry. Carelessness or failure in platform security can lead to significant consumer losses, damage to the industry's reputation, and threats to the stability of digital financial systems.

Regulation plays a crucial role in balancing innovation development and consumer protection. Arner, Barberis, and Buckley (2017) introduced the concept of "regtech and suptech" as modern solutions that help regulators monitor fintech innovations in real time.

At the international level, the PSD2 regulation in the European Union requires the use of Strong Customer Authentication (SCA) to reduce the risk of fraud in digital payments (Masi & Iannello, 2020). Additionally, GDPR strengthens consumer rights regarding personal data, including the rights to know, access, and delete their data.

RESEARCH METHOD

This research employs a qualitative, normative-juridical method that focuses on doctrinal legal analysis to examine consumer protection issues in digital payment systems and fintech-based credit services in Indonesia. A normative-juridical method is appropriate because the study centers on legal norms, statutory frameworks, conceptual doctrines, and comparative legal structures rather than empirical measurement. This approach allows the researcher to assess the adequacy, coherence, and effectiveness of existing regulations within the contemporary digital financial ecosystem (Soekanto, 2019; Marzuki, 2017).

4.1 Research Approach

To strengthen the analytical depth, the study integrates three complementary approaches within the normative-juridical framework:

a. Statutory Approach

The statutory approach is used to examine the legal norms governing digital payments and fintech credit both domestically and internationally. Primary legal materials include Payment Services Directive 2 (PSD2) in the European Union, relevant Bank Indonesia Regulations, Otoritas Jasa Keuangan (OJK) Regulations, and sector-specific laws concerning electronic transactions and consumer protection. This approach enables a structured evaluation of how far the existing regulatory framework fulfills its protective function for consumers (BI, 2022; OJK, 2023; European Parliament, 2015).

b. Conceptual Approach

The conceptual approach explores theoretical and doctrinal understandings of key legal concepts such as consumer rights, digital consent, algorithmic governance, transparency, and liability allocation in digital financial services. Through this approach, the research evaluates whether current regulatory concepts are adequate for addressing emerging risks in automated and data-driven financial technologies (Howells & Ramsay, 2020; Edwards, 2021).

c. Comparative Approach

The comparative approach assesses regulatory frameworks across multiple jurisdictions, including the European Union, United Kingdom, Singapore, and Indonesia. This approach aims to identify global best practices and highlight regulatory gaps or inconsistencies that hinder effective consumer protection in Indonesia. Comparison with mature regulatory environments provides a normative benchmark for evaluating Indonesia's regulatory adequacy and proposing reforms (Lynskey, 2019; Menon, 2022).

RESULT AND DISCUSSION

1. Indonesia's Consumer Protection Framework

1.1. Consumer Protection Act (UU No. 8/1999)

The Indonesian Consumer Protection Law, **Law No. 8 of 1999 on Consumer Protection**(commonly referred to as UUPK) serves as a fundamental legal framework safeguarding the essential rights of consumers. These rights include the right to comfort, security, and safety in the use of goods

and services; the right to accurate and honest information; the right to choose; and the right to compensation for losses. In the rapidly evolving landscape of digital payment transactions, the relevance of UUPK has significantly increased due to the transformation of consumer behavior and the shift from traditional offline transactions to highly integrated digital ecosystems.

Within digital payment services such as e-wallets, mobile banking, payment gateways, QRIS-based transactions, and fintech lending platforms service providers are classified as *business actors* (*pelaku usaha*) under UUPK. Consequently, they bear a legal obligation to ensure that all services offered meet adequate standards of security, reliability, and technological integrity. Business actors are strictly prohibited from disseminating misleading information related to service features, fees, interest rates, risks, or personal data processing policies.(Jain et al., 2023)

UUPK also establishes the principle of *product liability*, which assigns responsibility to business actors for any consumer losses resulting from negligence, system defects, operational disruptions, data-input errors, or unauthorized third-party use of consumer data. In the context of digital payments, such losses may include balance depletion, unauthorized transactions, digital identity theft, or non-transparent fee deductions. By imposing strict liability standards, UUPK reinforces preventive and corrective duties to protect consumers from both technological and operational risks inherent in digital services.

Although UUPK does not explicitly regulate electronic transactions given that it predates the digital economy the law has been progressively interpreted and enforced to encompass technology-based service models. In practice, UUPK operates in harmony with complementary legal frameworks, including the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and sectoral regulations issued by Bank Indonesia (BI) and the Financial Services Authority (OJK). This regulatory synergy strengthens UUPK's role as an overarching consumer protection umbrella, providing normative guidance for business actors while reinforcing principles of prudence, transparency, and accountability in all aspects of digital financial service delivery.

Accordingly, UUPK not only functions as a foundational statute but also as a harmonizing instrument that ensures consumer interests remain prioritized amid the innovation-driven expansion of Indonesia's digital payment and fintech credit ecosystem.

1.2. Electronic Information and Transactions Act (UU ITE)

Indonesia's **Electronic Information and Transactions Law**, **Law No. 11 of 2008**, as amended by **Law No. 19 of 2016** (commonly referred to as UU ITE) functions as the primary legal instrument governing the validity, security, and reliability of electronic interactions within the digital economy. The law

provides unequivocal legal recognition for **electronic documents, electronic signatures, and electronically formed contracts**, thereby establishing the foundational legitimacy of digital payment transactions and fintech-based lending agreements. This legal recognition is essential for ensuring that digital transactions possess the same binding force as traditional written agreements, thus supporting transactional certainty in an increasingly digitized marketplace.(JDIH BPK, 2022)

UU ITE imposes a series of obligations on **Electronic System Operators (ESOs)** which include digital payment providers, e-wallet operators, fintech lenders, banks operating online platforms, and payment gateway services. ESOs are required to implement robust systems that maintain the **confidentiality, integrity, and availability** of electronic information. These principles reflect globally recognized cybersecurity standards and represent the core pillars of secure electronic commerce:

1. Confidentiality requires ESOs to prevent unauthorized access to personal data, financial information, authentication credentials, and transactional records.
2. Integrity mandates the protection of data accuracy and completeness, ensuring that digital information and transactions are not altered, manipulated, or corrupted whether intentionally or through system malfunction.
3. Availability obliges operators to ensure reliable system performance, preventing service interruptions that could hinder consumer access to digital payment platforms or online financial services.

Violations of these obligations such as system failures caused by inadequate technological safeguards, unauthorized access resulting from weak cybersecurity protocols, or deliberate data manipulation may result in **administrative sanctions**, **civil liability**, and, in certain cases, **criminal penalties**. Administrative sanctions may include warnings, temporary suspensions, system shutdowns, or removal of non-compliant platforms from digital marketplaces. Civil liability allows consumers to seek compensation for financial losses or privacy violations, while criminal provisions may apply to cases involving fraud, hacking, illegal interception, identity theft, or intentional data breaches.

Importantly, UU ITE also intersects with the **Personal Data Protection Law (UU PDP)**, requiring ESOs to adopt transparent data processing policies, obtain lawful consent, and implement adequate security controls. When read together, UU ITE and UU PDP form an integrated normative structure that reinforces accountability among digital payment and fintech service providers, protects consumer rights, and enhances trust in Indonesia's digital financial ecosystem.

Through these provisions, UU ITE does not merely regulate electronic interactions; it establishes a comprehensive legal environment that obliges digital financial service providers to operate responsibly, securely, and transparently, thereby strengthening consumer protection in the rapidly expanding landscape of digital payments and fintech credit.

1.3. Personal Data Protection Act (UU PDP)

The enactment of Indonesia's **Personal Data Protection Law Law No. 27 of 2022 (UU PDP)** represents a transformative milestone in the nation's data governance landscape. As Indonesia's first comprehensive data protection statute, UU PDP aligns the country with global regulatory standards and responds to the increasing reliance on data-driven technologies within the digital economy. Digital payment platforms, electronic wallets, online banking applications, and fintech lending services all process vast volumes of sensitive personal and financial data, making the enforcement of UU PDP central to safeguarding consumer rights and ensuring trust in digital financial ecosystems.

A foundational principle of UU PDP is the requirement that personal data processing must be based on **legality, fairness, transparency, and purpose limitation**. This ensures that digital payment and fintech providers collect and process data only for legitimate, specific, and clearly communicated purposes such as identity verification, fraud prevention, credit scoring, or transaction authentication. The law prohibits excessive data collection, function creep, or repurposing consumer data without a lawful basis. This principle places substantive limits on platform operators that often engage in broad-scale data analytics, algorithmic credit scoring, or behavioral profiling.

UU PDP also introduces stringent requirements for **explicit consent**, particularly regarding **sensitive personal data**, which includes biometric information, financial data, transaction histories, and identification numbers. In the digital payment and fintech domain, the processing of such data is unavoidable; however, service providers must ensure that consent is obtained freely, is informed, and is capable of being withdrawn at any time by the data subject. This strengthens consumer autonomy and prevents coercive or opaque data practices that were historically prevalent in the digital finance industry.

In alignment with modern data protection frameworks, UU PDP provides consumers with extensive **data subject rights**, including:

- **Right of access**, enabling users to obtain information about their stored personal data and its processing activities;
- **Right to rectification**, ensuring consumers can correct inaccurate or outdated information, which is critical for credit scoring and KYC verification;
- **Right to erasure (right to be forgotten)**, allowing deletion of personal data when it is no longer necessary or when consent is withdrawn;

- **Right to restriction and objection**, particularly relevant where automated decision-making or profiling is used in fintech credit assessments.

These rights enhance transparency and give consumers meaningful control over their digital identities, while also compelling fintech and payment providers to implement responsive data governance mechanisms.

Given the global nature of digital financial transactions, UU PDP further regulates **cross-border data transfers**. Providers may only transfer data offshore if the recipient country or organization meets adequate data protection standards or if proper safeguards such as contractual clauses or binding corporate rules are implemented. This provision is particularly important for multinational payment processors, cloud service providers, and foreign fintech firms operating in Indonesia.

To ensure strict compliance, UU PDP establishes a robust enforcement regime that includes **administrative sanctions**, **civil liability**, and **criminal penalties**. Administrative sanctions may include warnings, fines, suspension of processing activities, or deletion of unlawfully processed data. Criminal sanctions apply to intentional misuse of personal data, unauthorized access, and illegal disclosure offenses that pose significant risks in digital payment environments where cyberattacks and fraudulent access are common.

Overall, UU PDP functions as a critical legal foundation for Indonesia's digital finance sector. It compels digital payment and fintech providers to adopt **privacy-by-design**, enhance cybersecurity, and embed accountable data governance practices throughout their operations. By elevating data protection standards, UU PDP strengthens consumer trust, supports sustainable innovation, and positions Indonesia to better integrate with international norms of data privacy and digital consumer protection.

1.4. Bank Indonesia Regulations (PBI) on Payment Systems

Bank Indonesia (BI), as the central bank and principal regulator of the national payment system, plays a pivotal role in safeguarding consumers in digital payment transactions. BI's regulatory framework is designed to ensure security, efficiency, interoperability, and consumer protection within the payment ecosystem. Several key regulations form the backbone of BI's approach:

a. Payment System Regulation (PBI No. 22/23/2020)

This regulation establishes requirements for **Payment Service Providers (Penyelenggara Jasa Pembayaran/PJP)**, mandating that operators implement **risk-management systems, fraud detection mechanisms, service continuity planning**, and adequate **cybersecurity controls**. It also requires providers to adopt **Know Your Customer (KYC)** procedures and maintain transparency in fee structures and service terms (Bank Indonesia, 2020).

b. QRIS and Standardization Framework

BI's standardization of QR-based payments through **QRIS (Quick Response Code Indonesian Standard)** reinforces consumer protection by ensuring interoperability, reducing fraud risks, and ensuring consistent security requirements across all providers (Bank Indonesia, 2019)

c. Consumer Complaint Handling and Dispute Resolution

The regulatory regime requires PJP operators to implement **accessible, transparent, and time-bound** complaint-handling procedures. BI also mediates disputes between consumers and providers when initial settlement mechanisms fail (Bank Indonesia, 2018).

Collectively, these regulations strengthen the resilience of Indonesia's digital payment infrastructure while ensuring that technological innovation proceeds alongside robust consumer protection.

1.5. OJK Regulations (POJK) on Fintech Lending

The **Financial Services Authority (Otoritas Jasa Keuangan/OJK)** regulates the broader fintech ecosystem, particularly **peer-to-peer (P2P) lending**, **digital financial innovation (IKD)**, and **digital banking**. OJK focuses on protecting consumers from **over-indebtedness, predatory lending, misuse of personal data, and technological vulnerabilities**.

a. POJK No. 77/POJK.01/2016 on P2P Lending

This regulation governs fintech lending platforms and requires providers to ensure:

- **transparent interest rates**,
- **risk disclosures**,
- **data privacy protections**,
- **responsible lending practices**, and
- **complaint-handling systems** (OJK, 2016).

P2P providers must also maintain data accuracy, prevent illegal debt collection practices, and provide secure storage of borrower financial information.

b. OJK Regulation on Consumer Protection in the Financial Services Sector (POJK No. 6/POJK.07/2022)

OJK regulation Number 6 and 7 of 2022 strengthens consumer rights by imposing:

- **obligations for fair treatment**,
- **clear and accurate information**,
- **prohibition of misleading marketing**,
- **enhanced data protection controls**, and
- **mechanisms for compensation** in case of provider negligence or system failure (OJK, 2022).

c. Digital Financial Innovation (Reg. No. 13/POJK.02/2018)

This framework ensures that fintech innovations undergo **regulatory sandboxes**, ensuring that new technologies such as algorithmic underwriting and open banking meet consumer protection requirements before deployment.

OJK's regulatory design emphasizes **transparency, accountability, prudence, and data stewardship**, aligning Indonesia with international best practices.

2. European Union Regulator Framework

2.1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is widely regarded as the most comprehensive and influential data protection framework in the world. It fundamentally reshapes how personal data must be collected, processed, stored, and transferred within the European Union and beyond. The GDPR is especially relevant to **digital financial services**, including digital payment platforms, e-money institutions, open banking systems, automated credit scoring, and fintech lending models that rely heavily on data-driven technologies.

2.1.1. Foundational Principles: Lawfulness, Fairness, Transparency, Purpose Limitation, and Data Minimization

GDPR establishes strict principles requiring that personal data must be processed **lawfully, fairly, and transparently**, and only for **specific, explicit, and legitimate purposes** (European Union, 2016, Art. 5). For digital payment providers and fintech credit platforms, this means data cannot be repurposed for marketing, profiling, or creditworthiness assessments without a lawful basis. The **data minimization** requirement further obliges financial service providers to collect only the data strictly necessary for transactional or regulatory purposes (Kuner, 2017).

This principle directly constrains common fintech practices such as excessive data scraping, behavioral profiling, or intrusive access to contact lists issues frequently observed in P2P lending ecosystems in emerging markets.

2.1.2. Strengthened Data Subject Rights: Access, Erasure, Portability, Objection, and Profiling Safeguards

GDPR grants consumers expansive rights over their personal data, including the **right of access**, **right to rectification**, **right to erasure ("right to be forgotten")**, and **right to data portability** (European Union, 2016, Arts. 15–20). In digital finance, these rights empower users to challenge algorithmic decisions related to credit

scoring, contest inaccurate financial records, and transfer their financial data to competing service providers.

The **right to object to automated decision-making and profiling** (Art. 22) is particularly relevant for fintech credit scoring models that rely on machine learning and big data analytics (Veale & Edwards, 2018). This ensures that consumers are not subject to opaque or discriminatory algorithmic determinations without meaningful human oversight.

2.1.3. Accountability and Data Protection Impact Assessments (DPIA)

A central innovation of GDPR is its emphasis on **accountability**, requiring data controllers and processors to implement technical and organizational measures demonstrating compliance. For digital payment operators, this includes encryption, pseudonymization, internal audits, access controls, and the appointment of a **Data Protection Officer (DPO)** under certain conditions (European Union, 2016, Art. 37).

Moreover, GDPR mandates **Data Protection Impact Assessments (DPIA)** for processing activities likely to result in high risks to data subjects such as large-scale transaction monitoring, open banking APIs, credit scoring, and fraud detection systems (Wachter & Mittelstadt, 2019). This requirement elevates consumer protection by ensuring that fintech operators assess and mitigate risks before deploying high-risk data processing technologies.

2.1.4. Mandatory Data Breach Notification Within 72 Hours

To address rising cybersecurity incidents in digital financial ecosystems, GDPR imposes a strict obligation to notify supervisory authorities of **personal data breaches within 72 hours** (European Union, 2016, Art. 33).

This requirement is highly consequential for digital payment platforms vulnerable to hacking, credential stuffing, or unauthorized access. Payment institutions must also notify affected users without undue delay when breaches are likely to result in financial loss, identity theft, or fraud. This transparency strengthens trust and enables consumers to take protective measures unlike jurisdictions where breach notifications remain discretionary or delayed.

2.1.5. Penalties and Sanctions: Up to €20 Million or 4% of Global Turnover

GDPR introduces some of the most severe sanctions in global regulatory history. Violations involving unlawful data processing, inadequate security, or unlawful cross-border data transfers may

result in administrative fines of **up to €20 million or 4% of a company's worldwide annual turnover**, whichever is higher (European Union, 2016, Art. 83).

Such penalties incentivize compliance among multinational fintech firms and digital payment service providers whose business models rely heavily on data monetization.

2.1.6. Extraterritorial Applicability: Global Reach Beyond the EU

GDPR's most transformative feature is its **extraterritorial scope**. The regulation applies to any organization regardless of geographic location that processes personal data of EU residents or offers goods and services to individuals in the EU (European Union, 2016, Art. 3).

This means that Indonesian **digital payment platforms, fintech lenders, data analytics companies, and cloud-based financial providers** fall under GDPR if they serve EU data subjects. Scholars widely recognize GDPR as a **global regulatory model**, influencing data protection reforms in Japan, Brazil, South Korea, India, and Indonesia (Greenleaf, 2018).

Its extraterritorial effect has prompted nations worldwide to emulate GDPR's structure, which explains why Indonesia's **UU PDP** shares conceptual parallels in lawful basis, consent, data subjects' rights, and cross-border data governance.

Through its robust principles, extensive rights, strong enforcement mechanisms, and global reach, GDPR forms a comprehensive framework that significantly shapes the consumer protection landscape in digital payments and fintech credit systems. Its influence is visible not only in EU member states but also in emerging markets seeking regulatory harmonization with global standards.

2.2. Payment Service Directive 2 (PSD2)

The **Revised Payment Services Directive (PSD2)** Directive (EU) 2015/2366 represents one of the European Union's most comprehensive regulatory reforms in the digital payments sector. Its primary objectives are to **enhance security**, **promote innovation**, and **strengthen consumer rights** within an increasingly integrated digital financial ecosystem (European Parliament & Council, 2015). PSD2 expands the scope of the original PSD (2007) by introducing new categories of regulated entities, reinforcing liability rules, and harmonizing consumer protection standards across EU member states.

A central element of PSD2 is the mandate for **Strong Customer Authentication (SCA)**, a security framework requiring multi-factor authentication for most electronic payment transactions. SCA significantly

reduces fraud by obligating payment service providers (PSPs) to verify users through at least two independent authentication elements knowledge, possession, or inherence (European Banking Authority, 2018). Studies have shown that SCA implementation has contributed to measurable declines in card-not-present fraud across the EU (Van der Linde, 2020).

PSD2 also lays the legal foundation for **Open Banking**, requiring banks to provide access to customer account data upon explicit consent via standardized Application Programming Interfaces (APIs). This enables **Third-Party Providers** (TPPs), such as Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs), to offer innovative payment and financial management services (Zetzsche et al., 2020). The open banking framework aims to improve competition by reducing the historical dominance of traditional banks and facilitating the entry of fintech companies.

In addition, PSD2 reinforces **consumer protection** by strengthening rules on transparency, liability, and dispute resolution. Consumers are insulated from losses due to unauthorized transactions, with liability typically capped at €50 when the payer has not acted fraudulently or with gross negligence (European Parliament & Council, 2015). The directive also mandates clear disclosure of fees, execution times, and currency conversion rates to ensure that consumers can make fully informed decisions.

Furthermore, PSD2 introduces **standardization across EU member states**, reducing regulatory fragmentation and promoting a unified digital payments market (EBA, 2021). Harmonized supervision supports cross-border interoperability and enhances the resilience of payment infrastructures.

Collectively, PSD2 reshapes the European digital payment ecosystem by balancing **innovation incentives** with robust **consumer safeguards**, making it one of the most influential global benchmarks for payment regulation.

2.3. Complementary Consumer Reglation

The European Union employs a multilayered regulatory architecture to safeguard consumers in digital markets, including those involving digital payments and fintech credit. Beyond sector-specific instruments such as PSD2 and GDPR, the EU's general consumer protection framework plays a crucial complementary role. These instruments ensure transparency, fairness, and redressability across online financial transactions.

2.3.1. Consumer Rights Directive (CRD)

The **Consumer Rights Directive (2011/83/EU)** strengthens consumer autonomy primarily through stringent **information disclosure requirements**, mandatory before the conclusion of any distance or online contract. Providers must clearly communicate pricing, fees, identity of the trader, withdrawal rights, digital content

functionality, and dispute-resolution options (European Parliament & Council, 2011).

In the context of digital payments and fintech credit, CRD ensures that consumers receive **accurate explanations of payment terms**, risk implications, automated decision-making processes, and potential charges, enabling genuinely informed consent (Howells, 2018). The directive also introduces a **14-day withdrawal right** for most distance contracts, providing consumers with a cooling-off period that reduces impulsive or uninformed financial commitments.

2.3.2. Unfair Commercial Praktice Directive

The **Unfair Commercial Practices Directive (2005/29/EC)** complements financial-sector regulations by addressing **misleading**, **aggressive**, and **opportunistic** business practices across all consumer markets. It prohibits deceptive representations regarding cost, risk, security, or functionality of digital payment services and fintech credit platforms (European Commission, 2016).

Scholars note that UCPD has become a crucial instrument for regulating **fintech marketing strategies**, particularly where digital lenders use persuasive design, behavioral nudging, or algorithmically targeted advertising (Micklitz & Winn, 2017). Enforcement authorities across EU member states increasingly apply UCPD against opaque pricing, misleading claims about credit approval likelihood, and non-transparent data-driven personalization.

2.3.3. Cybersecurity Standardization

Cybersecurity forms an essential part of the EU consumer protection landscape. Instruments such as the **NIS Directive (EU) 2016/1148** establish minimum cybersecurity standards for operators of essential services, including major digital payment infrastructures. Additionally, **ENISA** (the EU Agency for Cybersecurity) issues guidelines on secure API design, authentication, and incident reporting applicable to both banks and third-party fintech providers (ENISA, 2020).

These standards intersect with PSD2's Strong Customer Authentication (SCA) requirements, collectively ensuring that consumers benefit from **harmonized security protocols** and reduced systemic vulnerabilities (EBA, 2021)

2.3.4. Cross-Border Dispute Resolution Mechanism

Given the EU's integrated digital market, effective dispute resolution is essential. The **Online Dispute Resolution (ODR) Regulation (EU) No 524/2013)** provides a digital platform enabling

consumers to resolve cross-border disputes without litigation. Likewise, the **Alternative Dispute Resolution (ADR) Directive (2013/11/EU)** requires member states to ensure access to certified ADR bodies for disputes arising from online transactions (Hodges, 2019).

3. Comparative Analysis

3.1. Regulatory Structure

A fundamental structural difference between Indonesia's regulatory approach and that of the European Union lies in the **institutional architecture** governing digital payments, fintech credit, and consumer protection. The EU adopts a **harmonized supranational regulatory model**, while Indonesia relies on a **multi-regulator national framework**. These structural distinctions influence regulatory coherence, supervisory consistency, and the overall effectiveness of consumer protection in digital financial ecosystems.

3.1.1. The EU's Harmonized Supranational Model

The European Union operates under a system in which regulatory authority is **centralized and vertically integrated**. Key instruments such as the **General Data Protection Regulation (GDPR)** and the **Payment Services Directive 2 (PSD2)** apply **directly across all member states** without the need for transposition into domestic law (European Parliament & Council, 2016; 2018). This ensures a **uniform baseline** for consumer protection, cybersecurity, transparency, and data processing.

Moreover, the EU relies on supranational supervisory institutions such as coordinating enforcement of GDPR and providing binding guidance by **European Data Protction Borad (EDPB)**, issuing technical standards for PSD2 compliance, including Strong Costumer Authentication (SCA) by **European Banking Authority (EBA)** and initiating infringment actions againts member states failing to comply by The **Europe Commision**

This centralized structure significantly **reduces regulatory fragmentation**, enhances legal predictability, and strengthens cross-border consumer protection critical in a region where digital financial services routinely operate across national boundaries. Scholars describe this model as offering "coherent and interoperable protection standards unmatched by national regimes" (Micklitz & Reich, 2016).

3.1.2. Indonesia's Multi-Regulator National Framework

In contrast, Indonesia employs a **decentralized multi-agency system**. Regulatory authority is distributed across several institutions:

- **Bank Indonesia (BI)** – oversees payment systems, electronic money, QRIS, risk management, and system reliability
- **Otoritas Jasa Keuangan (OJK)** – regulates fintech lending, consumer protection in financial services, licensing, and governance
- **Kementerian Kominfo** – supervises electronic system operators (ESOs), cybersecurity obligations, and digital platform compliance
- **Ministry of Trade / BPOM (for specific cases)** – handle e-commerce and product-related safety issues
- **National Data Protection Authority (under UU PDP)** – handles personal data governance

These overlapping mandates often result in **regulatory fragmentation**, lack of terminological uniformity, and inconsistent interpretations across agencies (Susanto & Prabowo, 2023). The absence of a single supranational overseer, unlike the EU, means that Indonesia must rely on inter-agency coordination an area that remains operationally challenging.

Impact on Consumer Protection in Digital Payments and Fintech Credit The EU's centralized approach yields **stronger legal certainty and predictability** for consumers and service providers. GDPR ensures a single, harmonized data protection standard, while PSD2 guarantees consistent authentication rules, liability policies, and open-banking protocols across the internal market.

Indonesia's multi-regulator system enables **rapid innovation and flexible regulatory responses**, but it faces structural limitations, including:

- inconsistent enforcement intensity among agencies
- overlapping or ambiguous mandates
- fragmented consumer redress mechanisms
- lack of harmonized cybersecurity and data governance standards across sectors

As a result, consumer outcomes depend heavily on the specific sectoral regulator involved. For example, OJK's consumer protection framework for fintech lending is relatively mature, while BI's rules emphasize systemic stability and payment reliability, and Kominfo focuses on IT system security

and data processing compliance. This siloed architecture may weaken holistic consumer protection in integrated digital transactions, where payments, lending, data processing, and platform services overlap.

3.1.3. Harmonized Trends and Future Challenges

Indonesia has begun moving toward greater harmonization most notably with the enactment of the **Personal Data Protection Law (UU PDP)**, which adopts elements resembling GDPR. However, unlike the EU, Indonesia lacks a **single supranational coordinating authority** capable of enforcing cross-sectoral consistency. Thus, while Indonesia is adopting international best practices, full interoperability remains limited.

Scholars argue that adopting a more integrated supervisory structure possibly through a unified digital financial authority or enhanced inter-agency coordination mechanisms may be necessary to meet the complexities of modern digital ecosystems (Nasution, 2022).

3.2. Data Protections Standards

The **General Data Protection Regulation (GDPR)** is widely regarded as the world's most comprehensive and enforceable data protection framework. Its scope, precision, and enforcement mechanisms surpass those found in many national data protection laws, including Indonesia's **Personal Data Protection Law (UU No. 27/2022)**. While Indonesia's PDP Law adopts numerous GDPR principles such as purpose limitation, data minimization, consent requirements, breach notification obligations, and data subject rights important differences remain in terms of **regulatory independence**, **enforcement capacity**, and **penalty severity**.(Kartika Sari Ayumi, 2025)

Under GDPR, data protection is supervised by **independent supervisory authorities** in each EU member state, coordinated by the **European Data Protection Board (EDPB)**. These authorities possess extensive investigative powers, including the ability to conduct audits, issue binding decisions, order data processing suspensions, and impose administrative fines (European Parliament & Council, 2016).

Indonesia's PDP Law envisions a **Data Protection Authority (DPA)**, but the institutional structure remains partially integrated within the **Ministry of Communication and Informatics (Kominfo)** during its transition period. Scholars note that this transitional arrangement may undermine enforcement independence and may result in weaker oversight compared with EU institutions (Tisnanta et al., 2023). The absence of a fully autonomous

supervisory authority limits Indonesia's capacity to enforce high compliance standards comparable to those under GDPR

GDPR is internationally recognized for its **high financial penalties**, reaching up to **€20 million or 4% of global annual turnover**, whichever is higher (GDPR, Art. 83). These penalties have resulted in substantial enforcement actions against major multinational corporations, strengthening deterrence and encouraging strict compliance (European Data Protection Board, 2022).

By contrast, Indonesia's PDP Law imposes **significantly lower administrative fines**, generally capped at **2% of annual revenue** and subject to further implementing regulations. Criminal sanctions exist but are constrained by procedural thresholds. Scholars argue that the lower penalty framework may reduce deterrence, especially for large multinational platforms operating in Indonesia (Yuniarti & Sari, 2023).

Indonesia's PDP Law adopts these principles in a more **generalized and abstract** form, often requiring future implementing regulations to operationalize standards (Sihombing, 2023). This creates a compliance gap because many technical and operational requirements remain undefined.

Both GDPR and UU PDP guarantee core rights, including access, correction, erasure, and objection. However, GDPR provides **stronger procedural guarantees**, including the right to lodge complaints directly to an independent supervisory authority and the right to judicial remedies (Voigt & von dem Bussche, 2017). Indonesia's framework offers these rights in principle, but mechanisms for complaint-handling, mediation, and dispute resolution remain underdeveloped and partly dependent on ministerial administrative structures.

Indonesia's PDP Law adopts a similar tiered approach but lacks **detailed technical and contractual standards**, leaving cross-border compliance somewhat ambiguous pending full implementation.

3.3. Security and Authetication

A critical point of divergence between the European Union and Indonesia lies in the **authentication standards** imposed on digital payment service providers. Under the EU's **Revised Payment Services Directive (PSD2)**, Strong Customer Authentication (SCA) represents one of the most stringent and technically prescriptive frameworks for reducing fraud in electronic payment systems. In contrast, Indonesia's Bank Indonesia (BI) regulations adopt a more flexible, risk-based approach that lacks the granular, binding requirements found in PSD2.

PSD2 mandates **Strong Customer Authentication** for most electronic payments. SCA requires the use of **at least two out of three** independent authentication elements; something the user knows(e.g., password, PIN), something tHe user has(e.g., mobile device, token), something the user

is(biometric identifiers such as fingerprints or facial recognition.) (European Banking Authority, 2019)

These elements must be **mutually independent**, meaning that the compromise of one does not compromise the others. SCA is legally binding and enforced across all EU member states through EBA guidelines and technical standards (Zachariadis & Ozcan, 2017).

Studies show that SCA has significantly reduced fraud in online payments and card-not-present transactions, especially after the rollout of EMV 3-D Secure 2.0 (European Central Bank, 2020)

In Indonesia, authentication requirements are governed by several Bank Indonesia regulations, including PBI/22/23/2020 on Payment System Operators PADG 23/25/2021 and related technical guidelines.

Although these regulations require payment providers to maintain effective controls, BI uses a **risk-based approach** rather than prescribing mandatory multi-factor authentication requirements. Payment service providers must implement "adequate" security measures, but the standards are **contextual**, **non-uniform**, and often left to internal risk assessments by providers. (Kunci, 2025)

European Central Bank (2020) reports a **notable decrease in unauthorized online payments** following SCA implementation. Conversely, Bank Indonesia's semi-annual reports show that fraud incidents remain a major challenge in mobile banking and e-money platforms due to phishing, social engineering, and reliance on weaker authentication mechanisms (Bank Indonesia, 2022).

3.4. Transparency and Consumer Rights

A major point of divergence between the European Union and Indonesia lies in the **depth, specificity, and enforceability of consumer disclosure requirements** in digital payment services and fintech lending. While the EU imposes a **harmonized, legally binding, and granular** disclosure regime, Indonesia adopts a **sectoral, multi-regulator approach** that results in fragmented standards and inconsistent enforcement especially within the rapidly growing fintech lending sector.

Across its regulatory instruments including **PSD2**, the **Consumer Rights Directive (CRD)**, and the **Unfair Commercial Practices Directive (UCPD)** the European Union requires financial service providers to deliver **clear, comprehensive, and standardized information** prior to, during, and after a digital transaction.

The **Consumer Rights Directive (2011/83/EU)** mandates that such information be *"clear, comprehensible, and provided in a durable medium"* before contract formation (European Parliament & Council, 2011). Likewise, PSD2 requires transparent disclosure of **liability allocation**, **authentication procedures**, and **complaint-handling mechanisms** (European Commission, 2018).

The harmonized nature of EU law ensures that these disclosure obligations are not optional or subject to local interpretation. National regulators must enforce them uniformly, supported by supranational oversight from bodies such as the **European Banking Authority (EBA)**. Research shows that this regulatory clarity significantly enhances consumer trust and reduces information asymmetry in digital financial markets (Howells, 2018; Micklitz & Reich, 2016).

Indonesia's regulatory structure distributes consumer information requirements across **multiple agencies**, including OJK, BI, KOMINFO, UU perlindungan Konsumen (Consumer Protection Law.)

While each authority imposes certain disclosure obligations, none provides a **single, unified**, or **comprehensive** disclosure standard comparable to EU frameworks. Empirical studies show that many Indonesian fintech platforms fail to provide clear total loan cost disclosures, manipulate risk messaging, or obscure fee structures through non-transparent interfaces.(Waliullah et al., 2025)

3.5. Enforcement and Liability

Compared to Indonesia, the European Union's supervisory architecture under the **General Data Protection Regulation (GDPR)** establishes a *centralized and harmonized enforcement ecosystem* that strengthens accountability and accelerates regulatory response. The GDPR mandates the creation of **Independent Supervisory Authorities (SAs)** in each EU member state, coordinated through the **European Data Protection Board (EDPB)**, which issues binding decisions and ensures uniform application of the law across the Union (Voigt & Von dem Bussche, 2017; Kuner, 2020). This institutional design enables rapid coordination in cross-border cases, reduces regulatory uncertainty, and maintains a consistent interpretation of data protection standards.

In contrast, Indonesia's enforcement landscape remains **fragmented** across several authorities. Consumer protection violations may fall under the jurisdiction of the **Ministry of Trade**, **Badan Perlindungan Konsumen Nasional (BPKN)**, **Otoritas Jasa Keuangan (OJK)**, **Bank Indonesia (BI)**, and since 2022, the **Personal Data Protection Authority** under the Personal Data Protection Law (UU PDP). However, Indonesia has not yet fully operationalized a single, independent supervisory authority equivalent to the EDPB or national SAs, resulting in overlapping mandates, inconsistent sanctioning practices, and slower investigation timelines (Putri, 2023; Yudho & Sihombing, 2022).

The disparity in enforcement effectiveness can also be traced to differing **sanction regimes**. Under GDPR, supervisory authorities may impose administrative fines up to **€20 million or 4% of global annual turnover**, whichever is higher (GDPR, Art. 83). These substantial penalties create strong

deterrence effects and have been widely enforced, as seen in decisions against Meta, Amazon, and WhatsApp (EDPB, 2023). Indonesia's sanction framework while strengthened under UU PDP remains less robust, with lower administrative fines, limited enforcement precedents, and transitional regulatory capacities (UU No. 27/2022). This weaker deterrence contributes to slower compliance adoption among digital platforms and fintech operators.

Moreover, GDPR obligates controllers to implement mechanisms such as **Data Protection Impact Assessments (DPIAs)**, mandatory breach notifications within **72 hours**, and clear accountability obligations (Albrecht, 2016). Indonesia's PDP Law includes similar provisions but lacks the detailed guidance and secondary regulations that operationalize these obligations. As a result, compliance expectations are less granular, and enforcement remains reactive rather than preventive (Firmansyah & Lubis, 2023).

Overall, while Indonesia has made significant normative advances, the EU's centralized enforcement model under GDPR produces **more coherent regulatory action, faster cross-border coordination, and stronger accountability**, whereas Indonesia's divided institutional framework continues to generate **regulatory gaps, delayed enforcement, and inconsistent consumer protection outcomes** in digital payment and fintech credit ecosystems.

3.6. Extrateritoriality

Unlike Indonesia, the **General Data Protection Regulation (GDPR)** has a far-reaching **extraterritorial scope** that significantly shapes global data governance. Under **Article 3 GDPR**, the regulation applies not only to data controllers and processors established within the European Union but also to entities located outside the EU when they offer goods or services to EU residents or monitor their behavior within the Union (Kuner, 2020). This broad applicability has contributed to what scholars describe as the **"Brussels Effect"**, in which the EU's regulatory standards diffuse internationally because global companies adjust their practices to comply with GDPR across all jurisdictions rather than creating multiple compliance systems (Bradford, 2020). As a result, GDPR has become a de facto global benchmark for data protection, influencing regulatory developments in jurisdictions such as Brazil, South Korea, Japan, and Indonesia.

In Indonesia, however, the **territoriality principle** remains dominant. Laws such as the **Personal Data Protection Law (UU PDP)**, **Consumer Protection Law (UU PK)**, and **Electronic Information and Transactions Law (UU ITE)** apply primarily to data processing activities conducted within Indonesian territory or involving Indonesian citizens, but **do not explicitly adopt an extraterritorial model comparable to GDPR**. While UU PDP includes provisions on cross-border data transfers and the obligations of foreign electronic system operators providing services in Indonesia, its

operational scope depends heavily on implementation regulations and government-to-government cooperation (Hadi, 2023). This stands in contrast to GDPR's automatic applicability to foreign entities regardless of local registration or physical presence.

Practically, GDPR's extraterritorial reach imposes **binding obligations** on global fintech firms and digital payment providers such as conducting Data Protection Impact Assessments (DPIAs), appointing an EU representative, adopting strict consent mechanisms, and guaranteeing data portability (Voigt & Von dem Bussche, 2017). Failure to comply can result in severe fines, up to **4% of global annual turnover** (GDPR, Art. 83), making GDPR compliance a corporate priority even for firms operating outside the EU.

Meanwhile, Indonesia's territorial focus leads to **uneven enforcement** when foreign digital platforms and fintech providers access Indonesian users' data without local presence. Although the Ministry of Communication and Informatics (Kominfo) requires foreign Electronic System Operators (ESOs) to register, enforcement mechanisms remain limited, and administrative sanctions are considerably less stringent compared to EU enforcement practices (Putri, 2023). Consequently, multinational digital payment platforms may adopt **lower compliance standards** in Indonesia than in the EU, reflecting a **compliance asymmetry** shaped by regulatory incentives rather than technological necessity.

The divergence between the EU's universalistic regulatory approach and Indonesia's territorial approach creates broader implications for **consumer protection in digital payments and fintech credit**. In the EU, extraterritorial coverage ensures that consumers retain consistent rights such as erasure, rectification, and data portability regardless of where service providers are located (Albrecht, 2016). In Indonesia, however, consumers often face fragmented protections when engaging with cross-border fintech platforms, which may not be directly subject to domestic sanctions, resulting in **weaker accountability and limited legal recourse** in disputes involving foreign entities.(BPK JDIH, 1999)

Overall, the GDPR's extraterritorial scope not only elevates global compliance standards but also highlights the need for Indonesia to strengthen cross-border enforcement mechanisms, harmonize its data protection norms with international best practices, and establish clearer obligations for foreign digital service providers operating in its jurisdiction.

CONCLUSION

Indonesia has developed an increasingly robust regulatory framework to protect consumers in digital payment systems and fintech credit activities through a combination of statutory and sectoral regulations most notably the Consumer Protection Act (UU PK), Electronic Information and Transactions Law (UU ITE), Personal Data Protection Law (UU PDP), and a series of Bank Indonesia (BI) and Otoritas Jasa Keuangan (OJK) regulations.

Collectively, these instruments aim to provide a basic level of consumer rights, data security, algorithmic accountability, transparency, and complaint mechanisms within Indonesia's digital financial services ecosystem. Nevertheless, when compared with the European Union's more consolidated regulatory architecture, particularly the General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2), Indonesia's framework remains less integrated, sectorally fragmented, and comparatively weak in enforcement power and cross-border applicability.

Unlike Indonesia's sector-based model where BI and OJK regulate payments and fintech separately the EU adopts a comprehensive and harmonized approach that integrates data protection, payment system security, and market competition under a unified regulatory logic. GDPR establishes stringent rules for data minimization, explicit consent, algorithmic transparency, data portability, and high administrative fines, thus providing a strong foundation for digital consumer protection. Meanwhile, PSD2 complements this by mandating strong customer authentication (SCA), open banking standards, and clear allocation of liability across payment service providers. The harmonized nature of these frameworks creates an interconnected legal environment where consumer protection, cybersecurity, and financial innovation reinforce one another.

In contrast, Indonesia's protective framework, although significantly improved through the enactment of the PDP Law (2022), still faces substantive limitations. Enforcement relies heavily on administrative sanctions rather than punitive penalties, cross-border data governance is still evolving, and compliance obligations differ across financial sectors. While OJK and BI impose important obligations on fintech lenders and payment service providers such as transparency in fees, fair treatment obligations, and operational risk management these rules lack the holistic integration seen in the EU. As a result, consumer protection standards vary depending on whether a service falls under BI, OJK, Kominfo, or the general civil law regime, producing regulatory fragmentation that may reduce clarity for both consumers and digital service providers.

Furthermore, the difference in enforcement capacity is significant. The EU employs strong supervisory bodies with authority to impose fines that reach up to 4% of annual global turnover (under GDPR) or restrict operational licenses (under PSD2), which creates powerful incentives for compliance. Indonesia's enforcement mechanisms remain comparatively modest, with lower financial penalties and greater reliance on administrative warnings, system access restrictions, or revocation of licenses as a final resort. This disparity in regulatory teeth contributes to a gap in actual consumer protection outcomes EU consumers generally enjoy stronger rights related to privacy, dispute resolution, fraud prevention, and access to financial services.

Despite these differences, the EU model offers important lessons for Indonesia. Harmonization across regulatory bodies, stronger cross-border enforcement, clearer liability frameworks in digital payments, and greater algorithmic and data-processing transparency are areas with substantial potential for enhancement. Adoption of GDPR-style transparency obligations especially in automated decision-making within fintech credit scoring would help address concerns regarding opaque algorithms and potential discriminatory lending practices.

Similarly, PSD2-inspired open banking standards could promote innovation while ensuring consumer consent and security.

Strengthening these domains would not only enhance consumer confidence but also improve Indonesia's competitiveness within the global digital economy. As cross-border fintech services expand, alignment with international norms such as GDPR and PSD2 would facilitate interoperability, reduce regulatory arbitrage, and support long-term financial system stability. Overall, Indonesia's regulatory trajectory shows promising progress, yet meaningful integration, harmonization, and enforcement strengthening remain essential to achieving consumer protection standards comparable to the EU's mature digital regulatory ecosystem.

REFERENCES

Felstead, A., Jewson, N., Phizacklea, A., & Walters, S. (2002). Opportunities to work at home in the context of work-life balance. *Human Resource Management Journal*, 12(1), 54-76.

Fathni, I., Basri, B., Zulaika, S., & Dewi, R. S. (2023). Pengaruh Kebijakan Privasi, dan Tingkat Kepercayaan Pada Platform Digital terhadap Perilaku Pengguna dalam Melindungi Privasi Online di Indonesia. *Sanskara Hukum Dan HAM*, *2*(02), 118–126. https://doi.org/10.58812/shh.v2i02.305

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., &Tatham, R. L. (2006). Multivariate data analysis. Upper Saddle River, NJ: Pearson Education Inc.

Berry, W. (2005). War does not maintain peace or promote freedom. In L. I. Gerdes (Ed.), *War: Opposing viewpoints* (pp. 71-79). Detroit, MI: Greenhaven Press.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union.

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia, Japan, and South Korea. *Privacy Laws & Business International Report*, 151, 10–13.

Sujono, I., Baehaqi, J. F., Manullang, S. O., Rusli, M., & Dewi, R. S. (2024, March). Exploratory of cybercrime in law perspective, a research using bibliometric approach. In *AIP Conference Proceedings* (Vol. 2927, No. 1, p. 060044). AIP Publishing LLC.

Kuner, C. (2017). *The General Data Protection Regulation: A Commentary*. Oxford University Press.

Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398–404.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620.

BPK JDIH. (1999). *Undang-undang (UU) Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*.

Jain, R., Kumar, S., Sood, K., Grima, S., & Rupeika-Apoga, R. (2023). A Systematic Literature Review of the Risk Landscape in Fintech. In *Risks* (Vol. 11, Issue 2). MDPI. https://doi.org/10.3390/risks11020036

JDIH BPK. (2022). *Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Kartika Sari Ayumi. (2025). *Kebijakan Hukum Perlindungan Konsumen terhadap Kebocoran Data di Platform Fintech*.

Kunci, K. (2025). Tanggung Jawab Hukum Platform Fintech Dalam Menanggulangi Risiko Fraud dan Kejahatan Siber. *Blantika: Multidisciplinary Jornal*, *3*, 2025.

Waliullah, Md., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226–257. https://doi.org/10.63125/fh49gz18

Windani Sri, W. A. (2024). *IMPLIKASI HUKUM PERLINDUNGAN KONSUMEN DALAM TRANSAKSI KEUANGAN DIGITAL DAN PENINJAUAN PERATURAN PERBANKAN*.