http://ejournal.seaninstitute.or.id/index.php/Ekonomi
Jurnal Ekonomi, Volume 11, No 03 2022
ISSN: 2301-6280 (print) ISSN: 2721-9879 (online)

Digital Transformation of Banking and Its Legal Risks

Muhamad Agung Dharmajaya
STAI YAPATA Al-Jawami, Bandung, Indonesia

ARTICLE INFO

Keywords:
Digital Transformation, Banking, Legal Risk, Adaptive Regulation, Risk Mitigation.

ABSTRACT

Digital transformation of banking through the adoption of cutting-edge technology offers high efficiency, but on the other hand, it triggers the emergence of regulatory asymmetry (regulatory lag) and various new risk variants. This study aims to identify the dominant legal risk typologies in the era of banking digitalization and evaluate the readiness of the regulatory framework and effective legal risk mitigation mechanisms. The research method used is normative juridical with a descriptive-analytical approach to examine primary, secondary, and tertiary legal materials through literature review, which are then analyzed qualitatively using deductive reasoning. The results indicate three main legal risk typologies: violations of personal data protection due to data breaches, escalation of cybercrime such as phishing and ransomware that trigger disputes over unauthorized transactions, and legal uncertainty regarding the validity of electronic contracts (e-contracts) and the reliability of digital evidence in court. This study concludes that banks can no longer rely on unilateral exoneration clauses that harm consumers. Legal mitigation efforts must be implemented holistically by strengthening internationally standardized information technology governance (ISO 27001), strengthening e-KYC systems, implementing standard digital forensics audit logs, and utilizing cyber insurance. Meanwhile, regulatory authorities are required to shift their policy approach to principle-based, adaptive regulation to create a secure, trustworthy, and legally certain digital banking ecosystem.

E-mail:
agungdharmajaya456@gmail.com

1. INTRODUCTION

The development of information and communication technology in the era of the Industrial Revolution 4.0 has driven radical changes in various global sectors, including the financial industry. Digitalization is no longer merely a strategic choice to increase efficiency, but an absolute necessity for corporations to survive in market competition (Tarigan & Paulus, 2019). This phenomenon is forcing the traditionally rigid and bureaucratic banking sector to transform into a more dynamic, flexible, and digital-based one. This paradigm shift is completely changing the way financial institutions operate, interact with customers, and manage their business portfolios (Sumadi, 2020).

The digital transformation of banking is characterized by the mass migration of services from physical branches (brick-and-mortar) to integrated digital ecosystems (cyber-banking). The use of cutting-edge technologies such as Artificial Intelligence (AI), Cloud Computing, Big Data Analytics, and Blockchain is now a key pillar of modern banking operations (Kholis, 2018). Through these innovations, banks are able to offer mobile banking, internet banking, and even the establishment of fully digital banks (neo-banks). This innovation has successfully cut bureaucratic red tape, reduced operational costs, and expanded financial inclusion to even remote areas (Dz, 2018).

From a consumer perspective, banking digitalization offers unprecedented levels of convenience and speed. Customers can now open accounts, transfer funds across borders, apply for credit, and even invest in just minutes using personal computing devices (Novendra & Aulianisa, 2020). Transactions can be conducted anytime and anywhere, regardless of conventional bank operating hours. This ease of accessibility not only increases customer satisfaction but also triggers significant growth in the volume of national digital economy transactions (Rahmawati & Rahmawati, 2020).

However, despite the efficiency and convenience offered, the digital transformation of banking has the logical consequence of emerging new risk variants. The borderless and anonymous nature of cyberspace creates exponential vulnerabilities for the financial ecosystem (Samad, 2014). Risks that were once physical and local have now transformed into technology-based systemic risks that can occur within

seconds. The impact of these technological vulnerabilities not only causes direct financial losses but also creates complex legal implications for both banks and customers (Haryadi, 2007).

The most pressing legal risks in banking digitalization are threats to the security of customers' personal data and cyberattacks. Cases of data breaches, identity theft, and cybercrimes such as phishing, skimming, and ransomware continue to increase with the widespread adoption of financial technology (Latumahina, 2014). When sensitive customer data is exploited by irresponsible third parties, banks face civil lawsuits for unlawful acts. Furthermore, banks face severe administrative sanctions from supervisory authorities due to data protection system failures (Widiyasono, 2019).

Beyond data security issues, digitalization also triggers legal uncertainty in civil matters, particularly regarding the validity of electronic contracts (e-contracts) and the strength of digital evidence. The use of electronic signatures and facial recognition in banking transactions often gives rise to disputes in cases of default or fraud (Biondi, 2016). Traditional civil procedure often fails to address the authenticity and integrity of electronic evidence in court. Consequently, law enforcement in digital banking disputes remains unclear and complicates the process for parties seeking justice (Artanti & Widiatno, 2020).

This situation is exacerbated by the phenomenon of regulatory asymmetry, or regulatory lag, where the pace of financial technology innovation consistently lags far behind the development of written law. Current banking regulations are often reactive and unable to fully address the highly fluid operational dynamics of digital banks (Junaedi & Maulana 2014). This legal vacuum or delay in harmonization of sectoral regulations creates a gray area that endangers the stability of the financial system. Without solid legal certainty, digital banking innovation can actually turn into a source of economic anarchy (Saifudin, 2020).

Against this backdrop, in-depth research on legal risk mitigation in the digital transformation of banking is urgent and relevant. A comprehensive analysis is needed to map the boundaries of banks' legal responsibilities as service providers and customers' rights as consumers. This research plays a crucial role in bridging the gap between advances in financial technology and the need for equitable legal protection. The results of this study are expected to provide a roadmap for the banking industry in implementing legally compliant information technology governance.

Specifically, this study aims to identify the most dominant types of legal risks in the digital banking era. Furthermore, this study will evaluate the effectiveness of current regulations in mitigating these risks and formulate an ideal legal reconstruction concept. Through a normative juridical approach, this study is expected to provide theoretical contributions to the development of banking and cyber law. Practically, this study aims to provide policy recommendations for regulatory authorities and industry players to create a secure and legally certain digital banking ecosystem.

2. METHOD

This research employs a normative juridical approach (doctrinal law) that focuses on examining the principles, doctrines, and synchronization of written laws and regulations related to financial digitalization. The research is descriptive-analytical in nature, aiming to provide a systematic overview of the existing legal framework and identify legal gaps in digital banking operations. The data sources used are entirely secondary, classified into three legal sources (Diantha, 2016). Primary legal sources include banking sector regulations, laws on information and electronic transactions, and regulations on personal data protection. Secondary legal sources consist of scientific literature, legal journals, institutional research, and proceedings. Tertiary legal sources include legal dictionaries and encyclopedias to explain technical terms.

Data collection was conducted through library research using documentation techniques, namely reading, recording, and classifying legal sources based on their relevance to the legal risk issues of digitalization. All collected legal sources were then selected and analyzed qualitatively using deductive logic reasoning. This approach draws conclusions from general premises—in the form of legal norms, regulations, and monetary authority policies—toward specific premises related to cyber dispute resolution and legal risk mitigation in digital banks (Efendi, 2020). Through these analytical stages, this research produces a comprehensive, prescriptive, and argumentative descriptive presentation to address the legal issues raised.

3. RESULT AND DISCUSSION

Identification and Typology of Legal Risks in Banking's Digital Transformation

Digital transformation in the banking industry is not simply a shift from analog to electronic operational instruments, but rather a fundamental repositioning of the legal relationship between banks and customers. The integration of technology into banking business lines automatically gives rise to various

new dimensions of risk previously unknown in conventional banking law. Legal risks in this digital era are highly complex, cross-jurisdictional, and evolve exponentially following the pace of technological innovation. Therefore, identifying and classifying legal risk typologies is a crucial step for industry players and regulators to map legal responsibilities and prevent systemic failures that could undermine public trust.

The use of multi-platform technologies such as Artificial Intelligence (AI), Cloud Computing, Big Data Analytics, and Blockchain has become a key driver of efficiency in modern banking. However, the adoption of these third-party technologies poses legal risks in the form of technology supply chain vulnerabilities. When banks outsource data storage or transaction processing to cloud service providers or software developers, the boundaries of legal responsibility become blurred. If a third-party system failure causes a disruption to banking services, determining the legal culpability becomes a complex civil dispute between the bank, the customer, and the technology vendor.

The first and most crucial legal risk typology in the digital banking era is the risk of breaching customer personal data protection. Digital banks operate by collecting, processing, and analyzing sensitive customer data on a large scale for credit scoring and marketing purposes. This massive data processing activity places banks at high legal risk regarding personal data protection regulations. Any data processing carried out without the customer's explicit consent, or the misuse of data for purposes outside the agreement, constitutes a tort that can result in severe sanctions.

The real threat of data protection failures is data breaches due to hacker attacks or internal negligence. Legally, when customer financial and personal identity data is leaked to the public or traded on the black market, banks bear multiple layers of legal responsibility. Injured customers have constitutional and civil rights to file lawsuits for material and immaterial damages through the courts. Furthermore, under applicable personal data protection laws, banks also face the threat of substantial administrative fines, suspension of business activities, and even corporate criminal prosecution.

The second typology of legal risk is closely related to the escalation of cybercrime, which targets weaknesses in digital banking technology infrastructure and customer psychology. The anonymous, fast, and geographically barrier-free nature of digital transactions is exploited by criminals to launch large-scale cyberattacks. Cybercrime methods continue to evolve, from technical methods such as falsifying transaction data to highly structured psychological manipulation methods. The legal impact of these cybercrimes extends beyond the instant loss of customer funds to the damage to banks' legal reputations as trusted institutions obligated to safeguard the security of public funds.

One concrete manifestation of cybercrime risk is the emergence of legal disputes related to unauthorized transactions. Cases in which customer funds mysteriously change hands through digital banking applications often spark legal debates over who should bear the responsibility for the losses. Banks often shift responsibility to customers, claiming negligence in maintaining the confidentiality of passwords or OTP codes. Conversely, customers accuse banks of security vulnerabilities. The absence of clear standards of proof in assessing the reliability of the banking system makes the resolution of this dispute in court protracted.

Social engineering phenomena such as phishing, vishing, and impersonation are cyber threats that most frequently blur the boundaries of legal wrongdoing. In this mode, perpetrators manipulate customers into voluntarily providing confidential banking data. Normatively, a customer's act of providing access codes to another party can be categorized as a form of user negligence. However, under consumer protection law, banks are not automatically absolved of legal responsibility. Banks can still be held liable if proven to have failed to provide an adequate fraud detection system to detect unusual transaction activity.

In addition to targeting customers, cybercriminals also attack banking institutions directly through the distribution of ransomware malware. This attack paralyzes a bank's entire database and operational systems by locking access using high-level encryption and demanding a ransom. Legal risks arise when bank operations cease (system downtime), preventing customers from accessing funds or conducting important transactions. This failure to provide continuous service constitutes a clear violation of the principles of compliance and minimum banking service standards set by financial supervisory authorities.

The third typology of legal risks centers on material civil law aspects, particularly regarding the validity and interpretation of electronic contracts (e-contracts). In digital banking, agreement closing processes, such as loan applications or deposit openings, are conducted entirely online without face-to-face interaction. The legality of these digital contracts relies heavily on the validity of electronic agreements and digital signature mechanisms. Legal risks arise if the clauses in the e-contract are deemed vague, do not meet the requirements for a valid agreement, or contain hidden exoneration clauses that unilaterally disadvantage one party.

The digital customer identity verification process through the Electronic Know Your Customer (e-KYC) method using facial recognition technology also carries significant legal risks. Identity forgery using advanced artificial intelligence technology, such as deepfakes, has the potential to circumvent digital banks' e-KYC systems. If a bank approves the opening of an account under a false identity that is then used for money laundering or terrorism financing, the bank is legally deemed negligent in implementing the principle of prudence. Banks can be subject to criminal sanctions or severe administrative sanctions by financial intelligence agencies for this verification failure.

Legal uncertainty worsens when digital banking disputes enter the realm of procedural law in court. Traditional civil procedural law generally still prioritizes physical evidence in the form of written documents with wet signatures on paper. Although modern law has recognized electronic information as valid evidence, in practice, judges often struggle to assess the originality, integrity, and reliability of digital data submitted as evidence. Banks face the legal risk of losing a civil lawsuit if their digital audit log systems fail to meet digital forensic standards in court.

The borderless nature of cyberspace creates highly complex cross-border legal risks for digital banking. When electronic transactions involve foreign customers, foreign servers, or cybercriminals located abroad, determining which country's law applies (choice of law) and which court has jurisdiction (choice of jurisdiction) becomes a matter of international legal controversy. Disparities in cyber regulatory standards across countries often hamper law enforcement and the execution of court decisions, creating legal uncertainty that undermines the stability of the national banking industry.

Developments in blockchain technology and crypto assets are also encouraging banks to enter the decentralized finance (DeFi) ecosystem. This innovative approach creates significant compliance risk due to the immature and constantly evolving nature of digital asset regulations. Banks attempting to integrate their services with digital assets risk violating currency laws or capital market regulations if they misinterpret the legal status of these new financial instruments, which could ultimately undermine the bank's capital structure and the legality of its operations.

Regulatory Framework Readiness and Legal Risk Mitigation Mechanisms

A thorough evaluation of regulatory readiness reveals a norm gap triggered by the speed of financial technology innovation, which consistently outpaces legal development (regulatory lag). The current legal framework is often reactive and fragmented in responding to the highly fluid operational dynamics of digital banking. This creates a gray area that jeopardizes the stability of the national financial system and consumer protection. Therefore, legal reconstruction and cross-sectoral regulatory harmonization are needed to ensure that the digital transformation of banking has a solid and certain legal foundation.

The existence of umbrella regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP) has provided an initial foundation for the legality of cyber activities. However, in its implementation in the banking sector, these regulations still face challenges in synchronizing with technical regulations issued by financial supervisory authorities. Overlapping supervisory authority and differences in administrative sanction standards between institutions often confuse banking industry players in mapping their compliance frameworks, resulting in suboptimal law enforcement effectiveness.

On the other hand, technical banking regulations issued by financial authorities tend to focus on conventional prudential and risk management aspects, such as capital adequacy and liquidity. Regulations regarding cybersecurity standards, digital forensic audits, and electronic banking system reliability certification still require regular updates to remain relevant to evolving cybercrime methods. The absence of uniform national standard operating procedures for handling data breach incidents makes banking responses to cyber crises varied and immeasurable.

This regulatory asymmetry is increasingly evident in anticipating new business models such as fully digital banks (neo-banks) that operate without physical branch offices. Traditional banking law, which still adheres to the concept of physical presence, is hampered in overseeing these virtual entities. The limits of supervisory jurisdiction, determining a company's legal domicile for lawsuits, and even mechanisms for protecting customer funds in fully cloud-based banks are not comprehensively accommodated in current banking laws.

To address these regulatory weaknesses, the first legal risk mitigation mechanism the banking industry must adopt is to reconstruct the clauses in standard electronic agreements (e-contracts). Banks are no longer legally permitted to include exoneration clauses or standard clauses that unilaterally transfer all responsibility for system security to customers. The application of the principle of contractual fairness is absolutely necessary to prevent such clauses from being declared null and void by the courts under consumer protection laws.

In addition to contractual reforms, banking institutions are required to strictly implement internationally standardized information technology governance, such as ISO/IEC 27001 certification for information security management systems. Compliance with this standard provides banks with legal protection in court to demonstrate that they exercised maximum due diligence to protect customer data. This standard also serves as a mitigation tool to minimize the potential for civil lawsuits based on negligence in the event of a third-party cyberattack.

The next mitigation mechanism focuses on strengthening customer identity verification systems by integrating Electronic Know Your Customer (e-KYC) technology with official national population databases. Data validation, which is directly linked to civil registration authorities, minimizes the risk of identity fraud using artificial intelligence technologies such as deepfakes. By having a valid and certified verification system, banks can protect themselves from the risk of involvement in money laundering and terrorism financing that utilize fictitious accounts.

Banks must also implement a real-time fraud detection system supported by artificial intelligence and machine learning technology. This system analyzes customer transaction patterns and automatically blocks financial activity deemed unusual or suspicious. From a legal perspective, providing this proactive mitigation system is concrete evidence of the bank's fulfillment of its obligation to maintain the security of customer funds, while also facilitating the process of proving in court in the event of disputes over unauthorized transactions.

From a procedural legal perspective, digital banking needs to establish an audit log management system that meets international digital forensics standards. Every interaction, command, and transaction within a banking application must be recorded automatically, immutable, and accurately time-stamped. These electronic documents, managed to high forensic standards, will have perfect evidentiary power in court, thus overcoming unilateral objections from parties acting in bad faith.

Equally important mitigation measures include the transfer of legal and financial risks through the use of cyber insurance instruments. Given that no technological system is completely secure from hacker attacks, cyber insurance serves as a safety net to cover customer compensation costs, system recovery costs, administrative fines from regulators, and legal costs during court litigation. This step ensures that large-scale cyberattack incidents will not disrupt the liquidity and business continuity of banks systemically.

From a macro policy perspective, financial regulatory authorities need to shift their supervisory approach from a rigid and reactive approach to an adaptive and collaborative regulatory approach (adaptive regulation). The implementation of the regulatory sandbox method (isolated testing space) must be expanded to test every new financial technology innovation before its mass launch to the public. This mechanism allows regulators to identify and mitigate potential legal risks early without stifling the creativity and innovation of industry players.

Harmonization of international law is also an urgent mitigation agenda for regulators to address cross-border legal risks. The government needs to expand Mutual Legal Assistance agreements specifically for cybercrime and the exchange of encrypted financial data with other countries. This international jurisdictional cooperation facilitates the pursuit of banking cybercrime perpetrators who flee or operate their servers from abroad, and expedites the asset recovery process for customers.

At the operational level, increasing digital legal literacy within banks and the wider community is a highly effective preventative mitigation strategy. Banks are required to provide regular education to customers about the dangers of social engineering and how to maintain the confidentiality of banking access data. At the same time, improving the competence of law enforcement officials—including judges, prosecutors, and investigators—regarding the intricacies of digital banking law must be encouraged so that the legal dispute resolution process in court can proceed objectively and fairly.

4. CONCLUSION

The digital transformation in the banking industry has radically transformed the characteristics of operational risk into new, complex, systemic, and cross-jurisdictional legal risks. Research shows three primary legal risk typologies that dominate the current digital financial ecosystem. First, the risk of breaches of customer personal data protection triggered by data breaches in cloud-based storage systems. Second, the escalation of cybercrime such as phishing, social engineering, and ransomware, blurring the boundaries of culpability and triggering civil disputes related to unauthorized transactions. Third, legal uncertainty in the realm of civil procedure regarding the validity of electronic contracts (e-contracts), the validity of remote identity verification (e-KYC) methods, and the strength of digital evidence in court. The emergence of these three risk variants places banking institutions at multiple levels of legal threat, ranging

from lawsuits for damages based on unlawful acts, heavy administrative fines from supervisory authorities, to a massive erosion of public trust.

This situation is exacerbated by the phenomenon of regulatory asymmetry (regulatory lag), where conventional written banking regulations often lag far behind the pace of financial technology innovation. To address this challenge, the banking industry can no longer rely on exoneration clauses in standard electronic agreements to shift all responsibility for system security to customers. Ideal legal risk mitigation efforts must be implemented holistically by strengthening internal information technology governance that adheres to international standards such as ISO 27001, implementing a digital forensics-compliant audit log management system for evidentiary purposes in court, and utilizing cyber insurance instruments. Beyond industry players, regulatory authorities are also required to immediately reconstruct policies from their previously rigid and reactive nature to an adaptive, principles-based regulatory approach. This regulatory synergy is crucial for bridging the gap in norms, enforcing consumer protection, and creating a secure and legally certain digital banking ecosystem.

5. REFERENCES

Artanti, D. A., & Widiatno, M. W. (2020). Keabsahan Kontrak Elektronik Dalam Pasal 18 Ayat 1 UU ITE Ditinjau Dari Hukum Perdata Di Indonesia. *JCA of Law*, *1*(1).

Biondi, G. (2016). Analisis Yuridis Keabsahan Kesepakatan Melalui Surat Elektronik (E-Mail) Berdasarkan Hukum Indonesia. *Premise Law Journal*, *19*, 164959.

Diantha, I. M. P. (2016). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Prenada Media.

Dz, A. S. (2018). Inklusi keuangan perbankan syariah berbasis digital-banking: Optimalisasi dan tantangan. *Al-Amwal: Jurnal Ekonomi dan Perbankan Syari'ah*, *10*(1), 63-80.

Efendi, J. (2020). Metode Penelitian Hukum Normatif dan Empiris Edisi 1.

Haryadi, D. (2007). *Kebijakan Formulasi Hukum Pidana Terhadap Penanggulangan Cyberporn Dalam Rangka Pembaharuan Hukum Pidana di Indonesia* (Doctoral dissertation, program Pascasarjana Universitas Diponegoro).

Junaedi, E., & Maulana, I. (2014). Fraud Perbankan Syariah Dan Moralitas Keislaman. *Jurnal Asy-Syukriyyah*, *13*(1), 46-72.

Kholis, N. (2018). Perbankan dalam era baru digital. *Economicus*, *9*(1), 80-88.

Latumahina, R. E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya.

Novendra, B., & Aulianisa, S. S. (2020). Konsep dan perbandingan buy now, pay later dengan kredit perbankan di Indonesia: Sebuah keniscayaan di era digital dan teknologi. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 183.

Rahmawati, I., & Rahmawati, I. (2020). Analisis yuridis-normatif terhadap peran dan tindakan telemarketing dalam transaksi digital. *Jurnal Cakrawala Hukum*, *11*(1), 60-70.

Safudin, E. (2020). Harmonisasi Hukum dalam Antinomi Hukum (Analisis Terhadap Penerapan Pasal 20 Ayat 2 Huruf B Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman). *Al-Syakhsiyyah: Journal of Law and Family Studies*, *2*(2), 201-229.

Samad, A. N. (2014). Analisis Instrumen Cyber Terrorism Dalam Kerangka Sistem Hukum Internasional. *Universitas Hasanuddin Makassar*.

Sumadi, S. (2020). Menakar dampak fenomena pandemi Covid-19 terhadap perbankan syariah. *Jurnal Hukum Ekonomi Syariah*, *3*(2), 145-162.

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 294-307.

Widiyasono, N. (2019). Web Phising Attack Analysis on E-Commerce Service Using Network Forensic Process Method. *Jurnal Terapan Teknologi Informasi*.