Article │ Received 2 February 2026; Revised 22 April 2026; Accepted 27 April 2026; Published 28 April 2026
https://doi.org/10.55092/let20260004

Deconstructing the digital veil: criminal liability and ethical failures in AI-driven Sharia credit scoring systems in Indonesia

Rizaldy Anggriawan* and Muhammad Khaeruddin Hamsin

Faculty of Law, Universitas Muhammadiyah Yogyakarta, Bantul, Indonesia

* Correspondence author; E-mail: rizaldyanggriawan@umy.ac.id.

Highlights:

- Emergence of the digital veil.
- Shift in corporate criminal liability.
- Proposed Sharia AI audit framework.

Abstract: Artificial intelligence (AI) and Sharia banking are rapidly converging, resulting in fundamental transformations to the Indonesian financial system. A prime example of this convergence is the explosive growth of the buy now pay later (BNPL) industry. Whereas automated credit scoring can be leveraged to expand access to credit for consumers, it also raises important questions about financial inclusion *versus* creating a digital veil (*i.e.*, the algorithms used to score applicants) which may consist of a black box algorithm that is opaque regarding how it determines an individual's eligibility. As such, this form of automated scoring has raised concerns over the possibility of violating Sharia principles (e.g., clarity/tabyin, uncertainty/gharar). This study provides empirical and normative analysis of the inter-relationship between AI governance, Islamic juristic input, and the new Criminal Code of Indonesia (Law No. 1/2023). The findings indicate that there are likely to be algorithmic biases present, as well as willful blindness, by the management of these entities with respect to the corporate criminal liability standard applicable to the conduct of this opaque type of credit scoring system, which will render these entities subject to criminal fines of up to IDR 50 billion. Therefore, it concludes that Sharia-compliant banks must take proactive steps towards being Sharia-compliant in a digital manner by regularly conducting Sharia audits and using Explainable AI (XAI) for their automated systems, in order to ensure that the technical aspects of such systems remain consistent with the overarching objectives of Maqasid al-Sharia (higher objectives of Sharia).

Keywords: algorithmic bias; corporate criminal liability; Indonesia; Maqasid Al-Sharia; Sharia banking

1. Introduction

The financial landscape of Indonesia is in the middle of a structural transition as Sharia banking and the multi-finance sector become increasingly integrated with Artificial Intelligence (AI) and Machine Learning (ML). The non-bank credit performance has risen 7.77% year-on-year as of Q2 2025, while the amount of third-party funds in the banking sector has reached a historic high of IDR 9329 Trillion [1]. The fastest-growing segment within this rapidly growing market is the Buy Now, Pay Later (BNPL) segment. BNPL products offered through banks have increased by 21.03% in total outstanding credit amount in October 2025, and Multi-Finance providers saw an increase of 69.71% in total financing volume offered [2]. The rapid growth of BNPL products has been attributed to Automated Credit Scoring Systems (ACSS) that have been created to provide financial access to the so-called credit-undeserved. However, while ACSS systems provide increased access to credit through automation, they also create a digital veil, or an algorithmic black box that obscures the methodology used to validate transactions [3]. This includes the requirement for clarity and transparency of all transaction activities, as well as the principles of Islamic finance and the newly established framework for corporate criminal accountability under the reformed Indonesian criminal justice system.

Because of the way in which credit scoring has evolved from a human-based evaluation to an autonomous, algorithmic underwriting process, the risk of the technology is compounded by the theological mandate that governs Sharia banking. Under Sharia banking principles, the validity of any financial contract (Muamalah) requires that the contract not contain any riba (usury), maysir (gambling), or gharar (excessive uncertainty) [4]. Because machine learning algorithms that are currently in use are often black boxes, in that the algorithmic logic that was used to arrive at a conclusion cannot be accessed even by the institution's management, the adoption of such algorithmic systems negates the requirement for tabyin (clarity) and transparency of the contractual process. Additionally, when algorithms create algorithms that encode historical data bias, which results in systemic exclusion of marginalized groups or the imposition of exploitative profit margins based on proxy variables, such practices constitute not only an operational error, but also a crime of error, or Algorithmic zulm (injustice), against those who should be benefiting from the economic advantages of Sharia banking.

In Indonesia, AI's role in Islamic finance has been moving away from speculative claims and towards actual use. A recent study shows that both of these trends are becoming operational realities in Indonesia. For instance, Lasmiatun and Manteghi found that while AI has improved the banking sector's accessibility to data and improved the banking sector's use of data, there is still significant work to be done to align AI's black box nature with Sharia's prohibitions on gharar (excessive uncertainty) and riba (interest on loans) as outlined in the Qur'an and other Islamic texts [5]. Additionally, Al-Fatih *et al.* argues the implementation of AI credit scoring models has significantly reduced non-performing loan ratios across numerous institutions [6].

Despite the many advantages offered by AI credit-scoring models in terms of enhanced operational efficiency, however numerous institutions lack sufficient strategic capabilities to either successfully manage the ethical risks associated with utilizing AI technologies or to diversify their risk across multiple sources of debt. A growing number of studies are emerging that explore the intersection between technology and religious governance. Kamaruddin has developed an ethical framework grounded in the controversial principles of Maqasid Al-Sharia that asserts that Islamic finance should

not only focus on technical compliance but should also seek to promote the moral and spiritual development of the community in which it is conducted [7]. Haditama and Sugianto conducted a comparative analysis of corporate criminal liability. Their results illustrated that the absence of significant regulations regarding the use of AI creates an opportunity for corporations to use automated systems without fear of civil liability for their illegal actions [8].

While certain publications are beginning to examine the ethics of AI and corporate criminal liability in general, however the connection between algorithmic bias in Sharia credit scoring models, and the rigid corporate criminal liabilities set forth by the New Criminal Code in Indonesia (Law No. 1/2023) has not yet been made. Consequently, this paper offers a pathway for the transition from the conceptual discussion of the need for ethical guidelines to the practical implementation of such guidelines through the prosecution of corporate officers under the criminal law. This paper will specifically analyze and explore the significant implications of the ethically irresponsible actions of board members of Sharia banks who are found to be willfully blind to the fact that they employed biased algorithms in their credit-scoring models. This critical issue will not yet be captured by any current academic work until 2026.

While the urgency posed by the New Criminal Code's (2026) implementation for the Indonesian financial industry necessitates this research, this research also provides a roadmap for preventing Sharia Financial Institutions from exposing themselves to criminal liability. This research aims to analyze the theological and legal implications of algorithmic bias using the framework of the Maqasid Al-Sharia and identifies the requisites to establish a corporate criminal liability against AI systems that produce discriminatory credit outcomes. Finally, this research presents a Sharia AI Audit Framework as a means of establishing a standard of reasonable care or precautions under Indonesian Law.

The scope of this study is limited to Islamic compliant institutions in Indonesia with respect to their offerings of BNPL and automated credit scoring models. The study does not include conventional banking systems or any applications of AI outside of finance.

For clarity, the following terms will be used throughout this research. Digital Veil is a term used to refer to the legal metaphor relating to the inability of an individual affected by an algorithmic decision to understand the internal workings of an algorithmic decision-making system. It is important to differentiate the Digital Veil from Black Box because Black Box refers to the technical inability to interpret the algorithms used to make a decision. Furthermore, the term of Black Box refers to a machine learning model/pipeline that does not allow for the reconstruction or understanding of either the internal decision-making logic or the feature weights of the algorithm(s) used based on the available documentation or access. Meanwhile, Digital Mens Rea in this study refers to the legal concept that an organization's mental state(s) (e.g., willful blindness, systemic supervisory failures) can serve as a basis for holding the organization responsible for any harm caused by its automated systems. While the concept of Digital Mens Rea is not construed or suggested as an additional independent legal term, it is suggested as a method by which to apply existing legal concepts (e.g., organizational fault, negligence, willful blindness) to algorithm-related harms.

2. Methods

This study uses a normative legal research approach, with qualitative research of statutory regulations and Islamic legal theory supplemented by quantitative research of contemporary market data, to create a comprehensive understanding of how the New Indonesian Criminal Code, Law No. 1 of 2023, defines

Corporate Criminal Liability via Cumulative-Alternative Criteria as defined by Article 48 of the law. It is necessary to provide context in order to evaluate the intersection of digital finance standards with the emerging Criminal Mandates through an analysis of the OJK Regulations No. 29 of 2024 and No. 16 of 2025.

In addition to the above statutory analysis, the study incorporates an analysis of Theological Laws using and based upon Maqasid al-Sharia, or higher objectives of Sharia, to evaluate the ethical integrity of AI-driven systems. The study determines the categories of five essential protections, religion, life, intellect, lineage and property, and to assess how the specific technical risks associated with algorithmic bias and the risks associated with a lack of transparency, known as gharar, are mapped against these categories. The principles of tabyin and bayyinah are used in this process. The study is developing a normative legal structure of evidence to fill the gap between the lack of transparency of black box technology and the necessity of clarity in Islamic contracts.

The empirical-descriptive component of the research analyses 2025 market statistics related to the Buy Now Pay Later sector and the increasing number of non-performing loans. The synthesis of empirical evidence provides the basis for demonstrating the social/economic risks created by the current automated practices. Collectively, the statutory, theological and empirical approaches create the basis for proposing a Sharia AI Audit Framework which establishes a standard for reasonable preventive measures to avoid corporate criminal prosecution under the reformulated Indonesian legal system.

This empirical analysis takes as its base, the public aggregate market and regulatory data available (OJK booklets and press releases and national press reporting on the aggregate data for BNPL, along with industry press summaries) for the period between 2024–2025. The sources were selected on the following criteria: (1) relevance to BNPL/consumer credit within Indonesia; (2) availability to the public; and (3) recognition by Indonesian regulators. In preference to secondary publications or policy sources, primary statistical tables (covered by OJK) were utilized; however, contemporaneous press or secondary-policy materials provided context in the form of trends. Limitations: The empirical data is descriptive, showing trends and the levels of complaints by sector, and does not include micro-level data regarding individual loans or the results of model audits or other methodology used in generating algorithm models. Therefore, it is unable to provide evidence of any causal relationship between algorithm scoring and the levels of now pay later (NPL) or complaints reported. A discussion of these limitations is provided in further detail in the conclusions section of this work.

The paper will be divided into the following sections: The third section will give theological foundation, the fourth section will investigate statutory changes (art. 48), the fifth section will look at mens rea/willful blindness; and in the sixth and seventh sections, an examination of how liability should be distributed will be made. The eighth section will provide an empirical market context to show the social risk associated with AI; while the ninth and tenth sections will present a framework for Sharia AI Audit and conclusions.

3. The theological and jurisprudential grounding of algorithmic integrity

Integrating AI into Sharia Banking is not merely a technological integration; it must undergo thorough ethical review in terms of Maqasid al-Sharia (the higher goals of Sharia) before it can be adopted. Maqasid al-Sharia informs the Ethical Framework for A I for use in Sharia Banking will ensure that the five basic components of religion (Hifz al Din), life (Hifz al Nafs), intellect (Hifz al Aql), lineage (Hifz al Nasl), and

Property (Hifz al Mal) are protected [9]. Algorithmic bias directly contravenes these basic components through reinforcing social discrimination and therefore facilitating the Negative Act of devouring of wealth unjustly, (Surah An-Nisa (4:29).

Islamic legal theory uses the bayyinah (clear evidence) and gharar (excessive uncertainties) as barriers to the use of opaque algorithms. A contract will be deemed impermissible because of gharar if the degree of uncertainty is significant, the uncertainty relates to the object of the contract, and there is opportunity to avoid it [10]. If a Sharia Bank utilized a proprietary Credit Scoring Model that does not provide the consumer with an explanation as to how it determines the score, this would represent a significant gharar in the financing agreement, thereby making the material facts of the agreement obscure, potentially leading to the agreement becoming fasid (voidable) or batal (null and void).

An ethical evaluation of AI applications in Sharia banking must consider both the ethical principles of Maqasid al-Sharia as well as an analysis of how algorithmic technology relates to the theological mandates that guide these areas. For example, because algorithmic technologies may operate as "black boxes," it is possible that they could exacerbate social disparities and/or allow for the unjust "devouring of wealth." Both of these possibilities would violate the theological mandates associated with the protection of the five essential areas outlined in Maqasid al-Sharia. To demonstrate the ethical interactions between these two domains, Table 1 is used to illustrate how specific risks of algorithmic technologies (e.g. hidden riba, behavior manipulation) correspond to the legal and ethical restrictions that are applicable to each of the five essential areas established in Maqasid al-Sharia.

Table 1. Mapping Maqasid Al-Sharia to algorithmic vulnerabilities.

Maqasid al-Sharia Objective	Algorithmic Risk Factor	Legal and Ethical Implication
Hifz al-Din (Protection of Religion)	Integration of hidden riba or non-compliant structures in automated logic.	Violation of the sanctity of Sharia contracts; loss of institutional credibility.
Hifz al-Nafs (Protection of Life)	Economic exclusion leading to social instability or medical poverty among marginalized groups.	Failure of the bank's social responsibility to provide for human welfare (maslahah).
Hifz al-Aql (Protection of Intellect)	Manipulation of consumer decision-making through generative AI and deceptive nudges.	Erosion of human autonomy and critical reasoning, violating the principle of amanah.
Hifz al-Nasl (Protection of Lineage)	Gender or racial bias in underwriting that prevents family wealth accumulation.	Structural discrimination that undermines human dignity (karamah) and social justice.
Hifz al-Mal (Protection of Property)	Systemic financial loss due to discriminatory scoring or predatory hidden margins.	Reclassification as digital fraud or economic oppression (zulm).

Secondary analysis and sector reviews indicate that high rates of disparate bias within industrial AI systems have been reported (*i.e.*, one of the more often cited numbers would be "as high as 85%" within a specific set of industrial data); however, these kinds of estimates change dramatically depending on the domain and the quality of the dataset used to establish the estimate, as well as what definition is employed to define bias, therefore it should view these estimates as indicative and not definitive [11]. This is also apparent in the high growth of micro-financing and BNPL in Indonesia; AI algorithms are treating individuals in rural areas, or individuals with devices that are classified as low cost, as high risk in terms of creditworthiness when, in fact, the algorithms are perpetuating a system of geographic redlining that is completely contrary to the Sharia concept of 'adl (justice) [12].

4. The legislative paradigm shift: corporate criminal liability under law 1/2023

On January 1, 2026, Indonesia implemented its revised Criminal Code (Law No. 1/2023), which considerably modifies the nation's philosophy of criminal justice. Specifically, it combines the previously disparate sectoral statutes that imposed criminal liability on corporations into a single, comprehensive code [13]. As a result of this amendment, the Banking Sector, for example, will now have the ability to hold a corporation liable for its own criminal behavior within the context of that corporation's operations.

Pursuant to Article 48 of the revised Penal Code, corporations may be liable for the commission of a crime if any of the following cumulative-alternative criteria are met: (1) the act occurs during the course of the corporation's business activity; (2) the act results in an illegal benefit to the corporation; (3) the act is recognized as corporate policy; or (4) the corporation did not take reasonable precautions to avoid the commission of the act. In the area of Artificial Intelligence-based Islamic Banking, reasonable precaution will be the trigger for the prosecution of any bank that uses a biased algorithm and sustains a systemic financial loss or discriminates against its customers based on race or gender.

The provisions of Article 48 of the New Criminal Code create a list of alternative or cumulative bases for establishing the liability of corporations. A corporation can be held responsible for a criminal act performed in connection with that corporation's business activities; a corporation has received an illegal benefit; the corporation has adopted the criminal act as part of its corporate policies; and lastly, the person(s) representing the corporation did not take reasonable care to prevent the criminal act from happening. From a textual standpoint, the current provision reads as a fault-based provision and brings to light both omissions and failures to supervise; the most pertinent portion regarding algorithm-created harms will be how "reasonable precautions" are implemented within corporations, particularly with respect to management. Whether or not Article 48 creates a negligence standard or requires proof of an elevated degree of subjective intent is determined by both the statutory wording of the predicate crime and also what constitutes prosecutorial practice. In this area, most current literature supports the conclusion that prosecutors often rely upon evidence of both supervisory failures and corporation policies to demonstrate a corporation's culpability in the case of crimes based upon omissions.

If a banking organization uses, or has access to, a biased algorithm and suffers a systemic financial loss or engages in discriminatory pricing because it did not conduct algorithmic audits, adopt explainability protocols, or test for algorithmic bias, then that banking organization has arguably engaged in a criminal omission, which can serve as the basis for criminal prosecution under the New Penal Code (Law No. 1/2023).

The four alternative triggers for cumulative liability under Article 48 of Law No. 1/2023 for AI-based Sharia credit scoring are conceptual mapping based on operational and evidential contexts identified in Table 2. The first trigger (scope of business) establishes the relationship between the integration of an automated credit scoring system into a bank's normal business operations (the bank's primary underwriting function). The second trigger (unlawful benefit) occurs if an AI-based credit scoring system uses an algorithmic profile of vulnerable borrowers in order to establish profitable profit margins (ghaibi) from a group of borrowers who have limited access to traditional credit sources and could not afford to repay the high interest rates. The third trigger (corporate policy) can occur if the corporation's board of directors has established a policy favouring opaque efficiency over Sharia-compliant transparency, a

practice that could be evidenced via the minutes of the corporation's board meetings. The fourth trigger that seems to be the most critical in this situation (omission of prevention) is triggered by the lack of requirement for mandatory algorithmic auditing and/or the failure to take action on identified bias warning signs through the documentation required by OJK AI Governance Guidelines. Collectively, these four triggers provide a framework for determining that Sharia banks can meet all the elements required for a corporation to be prosecuted criminally based on algorithmic misconduct.

Table 2. Determinants of corporate criminal liability for algorithmic crimes (conceptual mapping with normative assessment).

Liability Trigger	Application to AI Systems	Evidence for Prosecution
Scope of Business	AI is integrated into the bank's primary credit underwriting and risk management.	Integration of automated scoring in the bank's Standard Operating Procedures (SOPs).
Unlawful Benefit	Predatory profit margins (margins ghaibi) applied to vulnerable groups identified by AI.	Financial reports showing anomalous profit gains from demographics with limited credit alternatives.
Corporate Policy	Management's prioritization of Black Box efficiency over transparency and Sharia compliance.	Board minutes reflecting the conscious decision to bypass explainability for speed.
Omission of Prevention	Lack of mandatory algorithmic auditing or failure to respond to bias warning signs.	Absence of documentation required by OJK AI Governance guidelines.

The New Criminal Code highlights that a 'preventative culture' should be embraced through proper use of Sharia compliant banking practices [14]. This requires Sharia banks to properly identify any existing gaps and reinforce their internal governance framework prior to the implementation date in January 2026. It also recognizes that misconduct can be facilitated by parties that exist outside of the formal structure of the institution; this can include de facto decision-makers and beneficial owners that may provide input into the design and implementation of an institution's AI technology.

5. Deconstructing the digital mens rea: willful blindness and algorithmic intent

An important issue confronting prosecutors in regard to AI crimes is the lack of criminals mens rea (Criminal Intent). Historically, the law has defined criminal intent as having a superior knowledge that only humans possess via moral awareness, which is absent in automated systems [15]. Nevertheless, the law in Indonesia is developing towards a collective or systemic fault model; whereby the criminal intent of an organizational entity is presumed by its organizational culture and supervisory failures.

The doctrines of willful blindness are two weapons available to prosecutors when establishing criminal liability for black box AI. The willful blindness doctrine states that an entity engages in willful blindness if they intentionally avoid being aware of certain facts or circumstances to escape responsibility for criminal conduct [16]. An example of willful blindness is with respect to the Sharia credit scoring example; if a board of directors believes they have no intent to discriminate against any group, then they cannot assert such a position if they had knowledge of the opaque or unclear nature of their vendor-supplied models and/or failed to investigate the high rejection rates for specific ethnic and geographic subgroups. Studies suggest that willful blindness is frequently relied upon in corporate fraud and financial misconduct as a strategy to avoid criminal liability, some multi-domain studies of corporate financial misconduct note that willful blindness features in a substantial minority of prosecutorial cases (estimates vary; some secondary accounts cite figures in the tens of percent) [17].

5.1. Modeling risk and accountability in Sharia AI

To quantify the threshold of criminal negligence, we can evaluate the risk of a Sharia Non-Compliance Event (R_{snc}) as a function of data bias (D_b), model opacity (M_o), and the failure of internal oversight (Ω):

$$R_{snc} = \sum (D_b \times M_o \times \Omega)$$

Where Ω represents the lack of reasonable preventive measures as defined under Article 48 of the New KUHP. If R_{snc} leads to a systemic violation of the Sharia prohibition of zulm (oppression) and results in an unlawful financial benefit, the corporate entity fulfills the elements of an economic crime. With the enforcement of the New Criminal Code, organizations are exposed to primary fines reaching up to IDR 50 billion for their silent acquiescence; secondary (even if passive) toleration of discrimination will also result in secondary sanctions (*i.e.* revocation of business licenses/corporate dissolution) [18]. The function presented above is a conceptual risk heuristic intended to map how technical, data, and governance factors interact to raise legal exposure. It is not an operational statistical model; below we suggest measurable proxies that could be used to operationalize it in future empirical work.

Operationalization suggestions:

D_b (data bias) → measurable by a disparate impact ratio or difference-in-approval-rate between protected *vs.* baseline groups.

M_o (model opacity) → measurable by an explainability score (e.g., percentage of decisions with feature-level explanations available).

Ω (oversight failure) → measurable by an oversight index (presence/absence of documented audits, frequency of tests, independent review).

6. Reconciling the black box with tabyin and the avoidance of gharar

Deep learning models are hard to understand, which is opposite of the Islamic concept of tabyin (clarity) and the prohibition of gharar (excessive uncertainty). Islamic Law offers an evidence-based solution to this issue in the form of a coherent evidentiary structure, based on bayyinah (evidence), qarīnah (circumstantial evidence), and amanah (trust), which can help mitigate the issues created by the lack of clarity (transparency) in AI. The AI does not provide absolute truths, only opportunities for corroborative evidence. To ensure that true and substantive justice is achieved, all AI-generated outputs should be subject to scrutiny by humans as an additional safeguard for the party that has the weaker bargaining power [19].

The Islamic prohibition of gharar in financial dealings is an important step to prevent injustice and to create parity or equity in business dealings, particularly for the party with weaker bargaining power. For example, algorithms used for creating credit scores create 3 forms of gharar in digital form; Technical gharar, which is created by mistakes in coding or hallucinations (false positives) that occur when using generative AI or systemic cyber vulnerabilities; Epistemic gharar, which is the lack of transparency in the logic behind the bank's or consumer's decisions regarding the credit scores; and Social gharar, which is created by the inability to predict how long-term effects of excluding persons automatically will impact the social/economic stability of the community.

To mitigate these digital gharar uncertainties, OJK Regulation No. 29 of 2024 on Alternative Credit Scoring (ACS) requires credit scores to have a statement explaining the basis for the score; however, the

current regulations have not developed specific standards for algorithmic explainability (XAI) or dataset representations and only contemplate a human-centric process of credit evaluations, which has created a regulatory lag and allowed discrimination to be hidden under the guise of the objective nature of the code.

Deep learning models have a lot of opacity, which results in three types of digital gharar: technical, epistemic, and social uncertainty. All three uncertainties provide ways to disguise discriminatory practices with the appearant objectivity of computer code through the creation of algorithmic zulm *i.e.* a form of injustice perpetrated against vulnerable populations, Table 3 outlines the means by which bias in the algorithm takes place within the financial sector in Indonesia. The table provides examples of historical encoding and proxy discriminations, specifically identifying the Sharia principles violated by the examples provided.

Table 3. Algorithmic bias mechanisms in Indonesian finance (conceptual taxonomy with Sharia implications).

Mechanism	Description	Sharia Violation
Historical Encoding	Models learn from past lending data that may reflect lower approval rates for rural or remote populations.	Reinforcement of zulm (injustice) and failure of 'adl.
Proxy Discrimination	Using variables like ZIP code or device metadata (older smartphones) as a proxy for low income.	Indirect discrimination and violation of hifz al-mal.
Behavioral Redlining	Analyzing social interactions or e-commerce patterns to classify individuals as high risk without direct financial evidence.	Introduction of excessive gharar and violation of consumer privacy.
Dynamic Pricing Bias	Algorithms sensing a consumer's lack of alternatives and raising prices/margins accordingly.	Predatory pricing violating the principle of mutual consent (An-Nisa 4:29).

7. The allocation of criminal liability: bod, dps, and developers

The main focus point of this research question revolves around who is responsible for criminal liability associated with systemic financial loss or ethical failure that has occurred as a result of an AI-driven Sharia product. Under Indonesian law, the responsibility for these events arises from three main actors; the Board of Directors, the Sharia Supervisory Board, and third-party developers.

7.1. The board of directors: fiduciary and operational accountability

Based on the regulations defined in Law No. 40 of 2007 regarding Limited Liability Companies, a Board of Directors could be held personally liable for any loss incurred by the company as a result of their actions, if they acted in error or negligence. The directors owe fiduciary obligations to the company and are bound to exercise the Duty of Care [20]. With regard to the use of AI in this regard, if a director acted with recklessness by deploying a scoring system that was not audited or used a biased approach to scoring that resulted in a breach of the regulations or consumer injury; the protective corporate veil may be lifted exposing the director to personal litigation or criminal prosecution.

In addition to the above, the Financial Services Authority's (OJK) Regulation No. 16 of 2025 establishes the obligations of the directors to pass a Fit and Proper Test and in addition; the OJK Regulation No. 16 of 2025 also requires that where a director has been found to have breached Sharia principles that such a finding is an impediment to their continued eligibility to serve as a director and therefore, will lead to their professional disqualification and possible criminal prosecution.

7.2. The Sharia supervisory board (dps): the crisis of professional liability

The DPS is responsible for ensuring Sharia compliance in all banking activities; however, their work is impeded by a competence gap in the fields of data science and digital finance [21]. Under the Islamic Banking Law No 21 of 2008 (Article 56), the DPS can be subject to administrative penalties for not properly applying the principles of Sharia law, while the Consumer Protection Law No. 8 of 1999 (Article 60) adds to this administrative penalty by also creating potential liability for professional or criminal levels of negligence in the performance of their oversight functions.

An example of this is that if the DPS does not request appropriate information about a bank's credit scoring systems or if the DPS rubber stamps a product that has hidden elements of riba or gharar, they may be deemed culpable based on the error known as unlawful acts (onrechtmatigedaad). Presently, the lack of interdisciplinary cooperation between Sharia scholars and AI engineers is the major challenge facing Sharia governance in the Indonesian fintech sector [22].

7.3. Third-party developers: vicarious and product liability

Often the AI technology used is obtained through licensing agreements with third-party vendors [23]. The absence of classic actus reus principles in relation to AI software, means the criminal liability must be around the people behind the technology, such as developers and service providers, through the application of vicarious liability [24]. To determine whether an algorithmic act meets the definition of actus reus, we must establish a direct connection between the algorithm's decision and the resulting harm (which may include, for example, discriminatory credit denials or predatory pricing schemes). In practice, this connection must be established through proof that the automated action significantly contributed to the resulting harm (for instance, e.g., proof may include audit trail information regarding the model outputs used to make Automated Decisions, quantitative data showing disparate impact across demographic groups, or documentation related to deployment of the algorithm). Thus, proving the actus reus of an automated process means combining the use of technical evidence from algorithmic logs and deployment records with more traditional forms of evidence.

The OJK Guidelines on Artificial Intelligence Governance for Indonesian Banks state that financial institutions, even when using licensed vendor models, have ultimate responsibility for results achieved through AI technology. This was prepared to complement various banks' acceleration of digital transformation that has been established by OJK, such as the Blueprint of Banking Digital Transformation, POJK 11/POJK.03/2022 on Information Technology Implementation by Commercial Banks, SEOJK 29/SEOJK.03/2022 on Cyber Defense and Security for Commercial Banks, SEOJK 24/SEOJK.03/2023 on Assessment of Commercial Bank Digital Maturity Rate, and Guideline to Digital Resilience. In addition, there could also be criminal liability for a developer who purposely builds an AI model that creates hidden margins or circumvention of Sharia law, which could result in being liable in the role of external actor or order-giver as defined under Article 47 of the New Criminal Code.

8. Empirical analysis: the BNPL surge and consumer risk

The need for reforms to improve the way banks provide and monitor their services is illustrated by the currently overwhelming number of consumers using services to purchase products through the use of a

financial product known as BNPL. As of August 2025, the total amount of money owed to banks through BNPL products was approximately Rp 24.33 trillion, and that number will continue to grow significantly over time. This rapid growth also shows how much more money can be borrowed through BNPL, with many people participating in this service. BNPL has especially grown rapidly through the growth of multi-finance companies, with a yearly growth rate of 79.91% in comparison to previous years. Along with this rapid growth comes an increase in the number of people who are not paying their loans (NPL), with NPL at 2.08% as of the first quarter of 2025 based on total system consumer loans [25].

While AI-based scoring improves the efficiency and speed of lending transactions, there is also data to support that it results in an increased reliance on a consumption-oriented model of debt, where 67% of all online loan debt goes to consumable purchases [25]. Furthermore, the growing number of consumer complaints being made about payment issues and about BNPL financing, shows that the current type of 'black box' lending practices is not able to deliver the required level of transparency and fairness that is expected of lenders by both OJK and Sharia law [26].

The rapid growth of the Buy Now, Pay Later (BNPL) industry has highlighted the need for regulatory reform. As an example, as of late 2025 BNPL accounts were holding around IDR 24.33 trillion of outstanding balances across banks. In addition to the growing balance, the rapid increase of BNPL is creating a creeping risk that has the potential for an increase in debt traps. This concern is evident based on the number of non-performing loans (NPLs) along with a staggering 379% year over year increase in the number of consumer complaints regarding BNPL products. Table 4 shows some market statistics for BNPL in 2025, including banking and multi-finance segments, in order to demonstrate the growing social and economic risk of BNPL.

Table 4. BNPL and digital credit market statistics (2025).

Metric	Banking Sector BNPL	Multi-finance BNPL	Combined Trend
Outstanding Balance	IDR 24.33 trillion	IDR 9.97 trillion	Surging debt levels (+21.03% banking yoy).
Annual Growth Rate	32.35%	79.91%	Acceleration in non-bank segment.
Number of Accounts	29.33 million	(Expansionary)	Massive digital onboarding.
NPF/NPL Rate	2.08% (System)	2.92% (Gross)	Creeping risk of debt traps.
Consumer Complaints	$1.1M Val. (2025)	(Significant portion)	379% yoy increase in complaint value.

9. Digital Sharia audits: a normative model for compliance

In order to tackle the issue of algorithmic bias and opacity, Sharia banks need to implement what has been termed intelligent Platforms, using AI, data analytics and Blockchain solutions as a means to provide evidence of compliance [27]. The proposed Digital-Trust Maqasidiyyah approach will allow Sharia banks to position AI and Blockchain technologies as supportive tools rather than as autonomous decision-making systems. The proposed Sharia Oracle will further enhance the ability of Sharia banks to use these technologies to improve the ethical character of Sharia contracts through adaptive smart contracts.

The research conducted thus far has shown that digital Sharia banking in Indonesia is currently sufficiently supported by legislation through the OJK regulatory framework and also has a progressive legal framework by way of DSN-MUI fatwas on products such as Islamic e-money and fintech lending [28]. The use of digital Sharia auditing for the purpose of automating compliance verification will greatly reduce the risk of human error or subjectivity in the audit process [29]. Additionally, Large

Language Models (LLMs), which can be trained in Islamic Fiqh (Islamic jurisprudence), can be used to perform real-time reviews of legal documents and fatwas to ensure Sharia compliance [30].

9.1. Proposed Sharia AI audit framework

The establishment of a Sharia AI Audit Framework is proposed to create a level of assurance for companies and the general public regarding the integration of Sharia principles into artificial intelligence technology. The following items comprise that framework: (1) Algorithmic Tadayyun—Divine values (*i.e.*, justice, fairness) are embedded within the design phase of the technology as optimization metrics; (2) XAI Mandate—to meet the principle of tabyin, Explainable AI must enable both auditors and consumers to better understand the reasons for rejecting/denying credit and/or the rationale for determining margin; (3) Dynamic Sharia Oracles—to address gharar (risk of uncertainty) for smart contracts, validation of the assets providing collateral using a blockchain-based oracle will provide real-time verifiability; (4) Bias Pressure-Testing—As one of the reasonable preventive measures under Law 1/2023, models must be stress tested for geographic/gender/socioeconomic bias.

The current conflict between technical regulation (OJK) and Sharia fatwas (DSN-MUI) must be harmonized in order to establish a cohesive governance framework—the absence of coordinated or harmonized standards stifles innovation while creating an environment of distrust amongst the public [31]. The application of a harmonization framework based upon Maqasid al-Sharia will ensure that the technical requirements for cyber resilience are equivalent to the normative requirements for financial justice [32].

10. Conclusion

The emergence of Artificial Intelligence in the field of Credit Scoring within Islamic Banking Institutions represents a significant opportunity for inclusion and fraud perpetration. The digital veil of the algorithmic systems has allowed for the establishment of systemic bias and unfair pricing through a system that is effectively exempt from traditional levels of oversight. Under the applicable provisions of Indonesia's New Criminal Code and the new OJK regulations, this study shows that, under certain circumstances, algorithmic bias may move beyond ethical concern and constitute a factor in regulatory or criminal exposure under the New Criminal Code, depending on the factual matrix and the presence/absence of documented preventive measures.

The determination by the two Boards of Directors and Supervisory Boards of Islamic Banks that algorithmic bias can be classified as digital fraud or economic discrimination will depend upon the failure of Banks to have implemented reasonable preventative measures. It will now be essential that Boards of Directors and Islamic Supervisory Boards understand that the concept of willful blindness toward the internal reasoning of the Banks' artificial intelligence systems will not provide a defense against criminal liability following January 2026. Therefore, the institutional accountability for Banks must be based upon the principles of tabyin, bayyinah, and the five purposes of Maqasid al-Sharia.

In order to ensure that Islamic Finance remains intact as we progress into the Digital Age, the country of Indonesia must shift from a theoretical frame of reference to one that has real-world implications through the application of digitally enabled Sharia Audits and Explainable AI systems. The growing number of unpaid loans in the BNPL sector along with the increase in consumer complaints illustrates the level of social and economic risk created by the banks' opaque (black box) decision-making

models. By dismantling the digital opacity and ensuring that each automated decision is reviewed against an ethical and fair standard of transparency, Sharia Banks can truly fulfill their commitments to provide all consumers with ethical and fair banking services. Sharia Banking will be developed going forward, not through the replacement of the ethical behavior of people with algorithms, but rather through the infusion of Islamic Jurisprudential principles into the programming of the algorithms.

Data availability statement

No supplementary or additional data were generated in this study.

Declaration of generative AI and AI-assisted technologies

The authors did not use generative AI or AI-assisted technologies in the writing of this manuscript.

Acknowledgments

The authors would like to express their sincere gratitude to Universitas Muhammadiyah Yogyakarta for the invaluable support and resources provided during the conduct of this research.

Authors' contribution

Conceptualization, Rizaldy Anggriawan and Muhammad Khaeruddin Hamsin; methodology, Rizaldy Anggriawan and Muhammad Khaeruddin Hamsin; formal analysis, Rizaldy Anggriawan and Muhammad Khaeruddin Hamsin; writing—original draft preparation, Muhammad Khaeruddin Hamsin and Rizaldy Anggriawan; writing—review and editing, Rizaldy Anggriawan; project administration, Rizaldy Anggriawan. All authors have read and agreed to the published version of the manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Financial Services Authority. Indonesia Banking Booklet 2025 Chapter 2: OJK's Authority Over the Banking Industry. 2025. Available: https://ojk.go.id/en/kanal/perbankan/data-dan-statistik/booklet-perbankan-indonesia/Documents/Pages/Indonesia-Banking-Booklet-2025/Indonesia%20Banking%20Booklet%202025.pdf (accessed on 14 January 2026).

[2] Virgiany M, Amatullah N. New OJK regulation on Buy Now Pay Later (BNPL) services. 2026. Available: https://www.hbtlaw.com/insights/2026-01/new-ojk-regulation-on-buy-now-pay-later-services (accessed on 15 January 2026).

[3] Mahmud MR, Hoque MR, Ahammad T, Hasib MNH, Hasan MM. Advanced AI-driven credit risk assessment for Buy Now, Pay Later (BNPL) and e-commerce financing: leveraging machine learning, alternative data, and predictive analytics for enhanced financial scoring. *J. Bus. Manage. Stud.* 2024, 6(2):180–189.

[4] Ichsan M, Fitriyanti F, Setiorini KR, Al-Qudah AM. Digitalization of Islamic banking in Indonesia: justification and compliance to Sharia principles. *J. Media Hukum.* 2024, 31(2):244–261.

[5] Lasmiatun KMT, Manteghi N. The impact of AI implementation on islamic financial literacy and global economic changes in the banking world. *J. Islamic Econ. Bus. Ethics.* 2025, 2(1):23–43.
[6] Al-Fatih S, Thahir PS, Muthohirin N, Ghapa N. Artificial intelligence in indonesia's financial sector. *Justicia Islam.* 2025, 22(2):303–326.
[7] Kamaruddin AM. Integrating Maqāṣid Al-Sharīʿah into Islamic Fintech: an ethical framework for sustainable digital finance in the era of Industry 4.0. *J. Innov. Creat.* 2025, 5(3):32277–32285.
[8] Haditama TK, Sugianto F. A comparative analysis of corporate criminal liability for AI-based malware: a study of indonesian and european union law. *Indones. Law Reform J.* 2025, 5(2):308–322.
[9] Asyiqin IZ, Alfurqon FF. Musyarakah mutanaqisah: strengthening islamic financing in indonesia and addressing murabahah vulnerabilities. *J.Media Hukum.* 2024, 31(1):1–18.
[10] Asyiqin IZ. Islamic economic law in the digital age: navigating global challenges and legal adaptations. *Media Iuris.* 2025, 8(1):95–112.
[11] Habib Z. Ethics of artificial intelligence in maqāṣid al-sharīa's perspective. *KARSA J. Soc. Islam. Cult.* 2025, 33(1):105–134.
[12] Wibowo BS. Regulatory challenges of ai-driven credit scoring in indonesian banking: between algorithmic bias and consumer protection. *Int. J. Multidiscip. Res. Anal.* 2025, 8(11):6525–6533.
[13] Butt S. Indonesia's new criminal code: indigenising and democratising indonesian criminal law? *Griffith Law Rev.* 2023, 32(2):190–214.
[14] Thalib P, Kurniawan F, Salsabila SM, Kholiq MN. Legal framework and employee liability in banking compliance and crime prevention: the case analysis of indonesia. *Yustisia J. Hukum.* 2025, 13(3):298.
[15] Osmani N. The complexity of criminal liability of ai systems. *Masaryk Univ. J. Law Technol.* 2020, 14(1):53–82.
[16] Acquaviva G. Autonomous weapons systems controlled by artificial intelligence: a conceptual roadmap for international criminal responsibility. *Mil. Law Law War Rev.* 2022, 60(1):89–121.
[17] Mustafa C. Addressing willful blindness: a multi-domain framework for enhancing legal accountability and fairness. *J. Hukum Peradil.* 2024, 13(3):551–584.
[18] Fajar R. Turning point for national criminal law: why corporations must understand Indonesia's new criminal code (KUHP 2026). 2026. Available: https://www.lawghp.com/files/Client_Alert_National_Criminal_Law_RF.pdf (accessed on 16 January 2026).
[19] Alhasan TK. Integrating AI into arbitration: balancing efficiency with fairness and legal compliance. *Conf. Resolut. Q.* 2025, 42(4):523–534.
[20] Saputra H. Legal liability of subsidiaries for unlawful actions committed by the parent company (holding company) in the structure of a limited liability company. *J. Law Polit. Humanit.* 2025, 5(6):4590–4598.
[21] Adinugroho M, Herlambang T, Hakiki MS, Yudianto F. The role of the Sharia supervisory board in Sharia banking in indonesia. *Islam. Bank.: J. Pemikir. Pengemb. Perbank. Syar.* 2023, 9(1):51–64.
[22] Muryanto YT, Kharisma DB, Ciptorukmi Nugraheni AS. Prospects and challenges of islamic fintech in indonesia: a legal viewpoint. *Int. J. Law Manage.* 2022, 64(2):239–252.
[23] Harrington JE. An economic test for an unlawful agreement to adopt a third-party's pricing algorithm. *Econ. Policy* 2025, 40(121):261–295.

[24] Fransisco W. Drafting laws for the lifeless: a legal framework for criminal liability and punishment for artificial intelligence. *J. Hukum Peradil*. 2025, 14(3):701–718.
[25] Estherina I. OJK: Indonesia's buy now pay later debt rises to Rp24.33 trillion. 2026. Available: https://en.tempo.co/read/2056509/ojk-indonesias-buy-now-pay-later-debt-rises-to-rp24-33-trillion (accessed on 18 January 2026).
[26] Abidin MI. Legal analysis of buy now pay later (bnpl) services and the urgency of consumer protection in indonesia's digital financial sector. *Braz. J. Dev*. 2025, 11(6):e80334.
[27] Alsaghir M. Digital risks and Islamic FinTech: a road map to social justice and financial inclusion. *J. Islamic Account. Bus. Res.* 2025, 16(7):1265–1282.
[28] Khasanah K, Arwani A, Said K, Ramadhan MUC. The pursuit of legal harmony in the integration of Sharia economic law compilation, ojk regulations, and dsn-mui fatwas. *Hikmatuna J. Integr. Islamic Stud*. 2024, 10(1):121–139.
[29] Khatib SFA, Abdullah DF, Al Amosh H, Bazhair AH, Kabara AS. Sharia auditing: analyzing the past to prepare for the future. *J. Islamic Accounting Bus. Res*. 2022, 13(5):791–818.
[30] El Amrani MY, Vakayil A, Mohammed F, Al Amri F. Foundations of domain-specific large language models for islamic studies: a comprehensive review. *J. ICT Res. Appl*. 2025, 19(1):69–85.
[31] Suaidi S. Bridging institutional and regulatory gaps: enhancing Sharia compliance in islamic financial institutions in indonesia. *el-Uqud J. Kajian Hukum Ekonom. Syariah*. 2025, 3(1):23–39.
[32] Azizov E, Azizov A, Azizli A, Babayev AA. A maqasid al-Sharia framework for fintech and digital asset regulation in muslim jurisdictions. *J. Islamic Law Legal Stud.* 2025, 2(2):96–113.