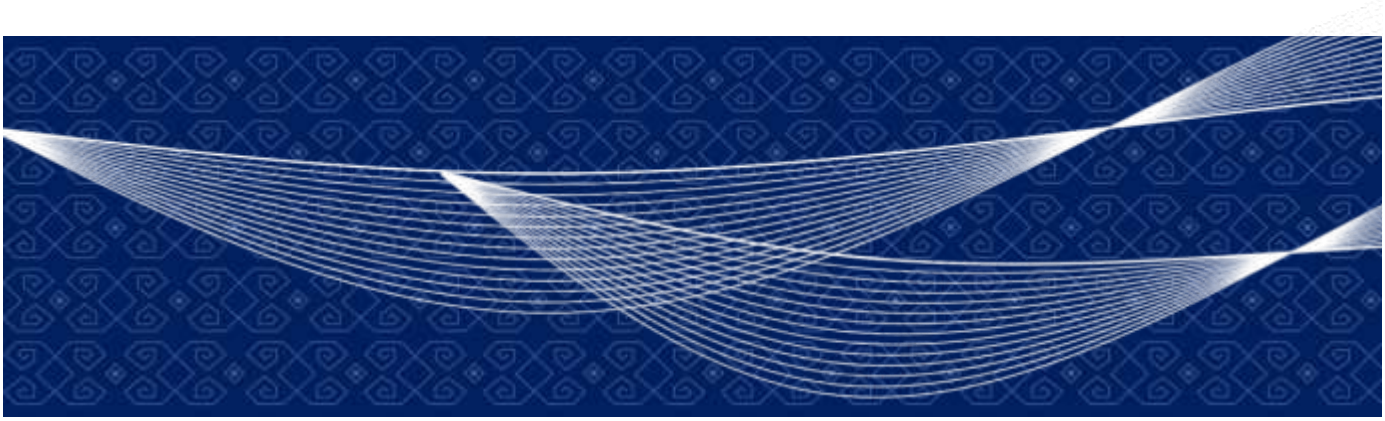
BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA



WP/20/2025

WORKING PAPER

THE ALGORITHMIC ALCHEMY: SYNTHESIZING GLOBAL LEGAL FRAMEWORKS FOR ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

Cicilia Anggadewi Harun, Safari Kasiyanto, Camila Amalia, Shinta Fitrianti, Esha Gianne Poetry, Nilasari, Rina Megasari, Naura Pradipta Khairunnisa

2025

THE ALGORITHMIC ALCHEMY: SYNTHESIZING GLOBAL LEGAL FRAMEWORKS FOR ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

Cicilia Anggadewi Harun, Safari Kasiyanto, Camila Amalia, Shinta Fitrianti, Esha Gianne Poetry, Nilasari, Rina Megasari, Naura Pradipta Khairunnisa

Abstract

This study examines and recommends regulatory and liability frameworks for the use of artificial intelligence in financial sector. Algorithmic bias, the black-box aspect of AI, data privacy concerns, and unequal treatment are the primary focus of this study. It employs normative, comparative, and empirical juridical analyses by assessing at AI-related laws and cases, comparing AI governance models across jurisdictions, and undertaking focus group discussions with academics, industry stakeholders, and regulators. For the comparative analyses the study evaluates the regulatory models and AI-related cases in the European Union, the United States, Singapore, Australia, China, and Qatar. The result shows Indonesia should use a hybrid model that begins with an adaptive sandbox phase, moves toward a risk-based framework to balance innovation and responsibility, and subsequently transitioning to a co-regulatory model as AI utilization escalates. Additionally, considering that AI is a non-legal subject, the proposed Clear Box Liability framework puts a strong emphasis on human accountability through proportional liability principles. Furthermore, the FairSight Liability Model strengthens consumer protection, transparency, and effective dispute resolution in AI-driven financial services by integrating fairness and foresight.

Keywords: Artificial Intelligence, AI Regulatory Framework, AI Bias, Consumer Protection, AI in Financial Services, AI Liability Framework

JEL Classifications: A11, B11, C11, D11, F11,

1. Introduction

The use of Artificial Intelligence (AI) and Machine Learning in the financial system has emerged as a transformative force and offering potential benefits. While these technologies are powerful, their application in financial system can often be opaque to both financial agents and consumers. The lack of transparency in AI algorithms creates a significant information asymmetry between tech companies that develop these systems and the consumers who rely on them. This opacity raises concerns about bias and fairness, particularly when it comes to decision-making processes that affect consumers' financial well-being.

Both the financial agents and the consumers could take advantage of using AI. The financial agent can deploy a more rigorous credit assessment and better customer identification, gather more information to analyze the market, and in turn develop more marketable and profitable products. AI can also help reduce risks that come from potential fraudulent attempts and cyber-attacks. The customers can experience faster financial services, personalized financial products and better liquidity, and investment management. In more than one way, AI/ML also allows financial agents to merge their services with other types of financial institutions and even non-financial institutions and subtly go beyond the regulatory barriers.

The use of AI/ML in the financial system also has brought the financial agents and customers into the world of AI/ML that is opaque for them. Some of the best financial startups were led by information technology professionals. They control the algorithm and guide the development of the application with their savviness in the computer world. The financial agents and the customers do not necessarily understand the algorithm in general. This means that most of the time financial agents and customers use the application without knowing how the algorithm works. This poses asymmetrical information between tech companies and consumers. Risk mitigation concerning the opacity of the AI algorithm has become an increased concern for authorities.

For reasons caused by the opacity of AI designs and processes, consumers were sometimes unaware of how their personal data is used in the applications. Machine learning is very data hungry and potentially becomes smarter from feeding financial transactions and consumers' responses to the applications. The application can run in the background to process consumers' data. It could be in the form of financial transactions, profile information, and patterns of responses to the application, more often than none with the absence of consumers' consent. The information is then used to decide for the consumers, to generate new offers or generate marketing strategies to lure other consumers to participate in the AI application.

Human decision-making can produce biased outcomes, as choices are shaped by automatic emotional responses or controlled cognitive processes (Greene et al., 2008). In many cases, we cannot identify which consideration dominated a past decision, making it an unknown variable that still influences historical records. Since AI/ML models rely on these past decisions as training data, the systems can inherit and reproduce such biases becoming the first major source of bias in AI/ML. Developers may or may not be aware of this risk. As a response, explainable AI (XAI) is increasingly used to clarify model behavior, expected impacts, and potential biases, helping maintain financial system integrity amid rising AI adoption.

Another source of bias arises when developers intentionally embed certain considerations into an algorithm whether to target specific market segments or to prioritize particular factors. For instance, a driverless car trained mainly on simulated scenarios may miss real-world human interactions, leading to incomplete decision rules. In such cases, customers should be informed, and all risks stemming from limited testing must be disclosed. Transparency in AI/ML algorithms must be upheld regardless of these limitations.

In terms of the implementation of AI, Indonesia presents a unique AI landscap, it is one of the world's largest and most receptive digital markets, ranking high in AI usage,

Yahoo!Tech even places Indonesia eighth in AI tool website visits. However, the country consistently scores low in AI literacy, making users vulnerable to privacy breaches, bias, opaque algorithms, fraud, and cyber risks. Industry representatives note that no major customer-triggered cases have emerged, not because the risks are absent, but likely due to low awareness and limited understanding of AI among Indonesian users.

Global frameworks like the EU's GDPR and China's algorithm regulation emphasize transparency and accountability in AI use. Indonesia's Personal Data Protection Law mirrors many GDPR principles and, together with the Consumer Protection Law, forms the basis of consumer protection in AI-driven financial services. However, current regulations still fall short in addressing AI-related challenges especially bias, liability, and mechanisms for resolving disputes arising from biased or opaque AI decisions.

This paper examines whether Indonesia's regulatory framework sufficiently mitigates bias in AI-supported financial decision-making, beyond existing data privacy protections. It explores how conflict resolution, liability, and institutional responsibility, particularly for Bank Indonesia in safeguarding payment system integrity should be structured. Using normative, comparative, and empirical (FGD-based) juridical methods, the study evaluates global practices and proposes improvements for Indonesia, including stronger liability rules, clearer consumer protection mechanisms, and enhanced AI literacy.

The paper is expected to contribute to addressing the regulatory gap in the use of AI in Indonesia's financial sector to safeguard consumers by proposing a regulatory framework, including a liability framework. It also argues the importance of collaborative forums between regulators, AI developers, and consumers to explore AI bias and conflicts resolution. The study is also expected to develop an adaptive regulatory framework that ensures consumer protection, including against AI bias, accompanied by effective conflict resolution mechanism

Chapter 2 provides a literature review on the implementation of AI/ML in financial systems, along with a comparison of regulatory frameworks across various countries. Chapter 3 outlines the research methodology. Chapter 4 discusses the gaps in the current regulatory and liability frameworks and proposes recommendations for improving consumer trust in AI/ML applications. Finally, Chapter 5 concludes with the findings and recommendations.

2. Literature Review

2.1. AI Implementation and Potential Risk of Bias in AI Implementation

The use of AI, including ML and Generative AI (GenAI), has grown rapidly, particularly within the financial sector. As these technologies advance, the financial industry is increasingly leveraging AI to enhance operational efficiency, streamline decision-making processes, and foster innovation in product and service offerings. According to the 2020 McKinsey Global Survey, the financial and banking sectors rank third in terms of AI adoption, following the telecommunications and automotive industries (Herman, H., & Masawi, B, 2022). AI has significantly transformed the financial industry by supporting financial institutions in both internal business processes and customer-facing services.

The use of AI in the financial sector can be divided into various areas that support increased efficiency and service quality. One example is applications that are directly related to customers. The most common application is chatbots that function to interact with customers directly. AI-powered chatbots can provide instant customer service, handling various questions, requests, or complaints without the need for human intervention. This not only improves operational efficiency but also enhances customer experience by providing fast and accurate responses. In addition, AI also contributes greatly to Know Your Customer (KYC) and personalization or customized product proliferation. Using algorithms that analyze big data in real-time, AI enables related

financial systems to identify customer preferences, habits, and specific needs. Thus, it can provide services and products that are more tailored to the individual characteristics of customers, thereby creating a more personal and relevant experience. For example, customers can receive more appropriate product recommendations or financial solutions that suit their financial conditions. The application of AI in digital banking is also becoming more profound, utilizing technology to enhance customer experience through faster, more efficient, and more responsive digital application-based services. AI enables banks to simplify transaction processes, speed up payment authorizations, and provide more accessible services.

In risk management, AI has been effectively utilized in payment systems to detect fraud and assess financial risks. AI technology enables financial institutions to analyze large volumes of transaction data in real-time, allowing them to identify suspicious transaction patterns more accurately and quickly compared to traditional methods (Beytollahi & Zeinali, 2020). The use of ML in fraud detection significantly enhances operational efficiency and reduces the risk of fraud. With ML's ability to learn transaction patterns and identify anomalies based on historical data, the system can provide early warnings and prevent high-risk transactions. Furthermore, AI helps financial institutions address more complex challenges, such as money laundering and cybercrime, which are becoming increasingly sophisticated with the digitalization of the financial sector. By improving accuracy and speed in fraud detection, AI plays a critical role in strengthening the security and risk management capabilities of financial institutions, making them more responsive to emerging threats (Canhoto, 2021).

AI applications are also used as predictive analytics tools that utilize algorithms to analyze large datasets with the aim of predicting market trends, assessing credit risk, and optimizing investment portfolios with greater accuracy. This technology enables financial institutions to identify patterns more effectively and efficiently than traditional methods, thereby providing deeper and more adequate insights for decision making. In terms of credit scoring, AI is used to analyze larger datasets, including consumer data, to understand behavioral patterns and financial characteristics. Predictive analysis in this case predicts the likelihood of default, as well as performing feature selection and optimization, thereby providing a more accurate assessment of a customer's creditworthiness (Bhatore, Mohan, & Reddy, 2020).

AI use in the financial sector not only improves operational effectiveness and efficiency, but also presents risks that need to be considered, particularly those related to bias in AI systems. In the AI life cycle, data and learning algorithms are the main sources that determine the quality and accuracy of output. Therefore, the application of AI in the financial realm must be supported by representative data and transparent algorithms to minimize potential bias. Data bias occurs when the data used to train algorithms does not reflect the actual population, resulting in models that produce unfair decisions. Meanwhile, algorithmic bias arises from the design and architecture of the algorithm itself, for example when algorithms reinforce existing injustices in the data or make decisions that are difficult to explain transparently.

In the case of AI used in financial systems, errors or bias can easily occur. In credit scoring, two of the main issues are data and algorithmic bias. It is a condition where AI models inherit and reinforce historical biases found in training data (Adewale et al., 2022). If previous credit decisions were influenced by systemic discrimination, AI models can perpetuate unfair lending practices that disproportionately affect minority groups and low-income individuals (Adewale et al., 2022). This raises ethical concerns regarding fairness and the potential for discriminatory outcomes, even if lenders do not explicitly intend to discriminate against. Unlike traditional credit scoring methods, which are relatively explainable, many AI models operate as black-box systems, making it difficult for customers to challenge adverse decisions or identify errors in the assessment process.

Several real-world cases highlight these risks. For example, a widely used AI lending algorithm systematically assigned lower credit limits to women than to men, and certain racial groups were unfairly blacklisted from the system based on negative historical data,

even when their financial profiles were identical, sparking public outcry and regulatory scrutiny. Another example is an AI-based loan approval system that inadvertently disadvantaged applicants from low-income neighborhoods. The model, trained on historical data, reinforced existing biases by assigning higher credit risk based on geographic location rather than individual financial behavior. These cases underscore the dangers of algorithmic bias in AI-based credit scoring (Antonevics, 2023).

Other implementations in AI-based fraud detection systems offer significant improvements in identifying suspicious activity and reducing financial losses. Traditional fraud detection systems rely on rule-based mechanisms and manual inspection, thus often produce false positives and delayed fraud detection. Meanwhile, AI models such as Natural Language Processing (NLP) allow for real-time pattern identification and anomaly detection, thus facilitating active and adaptive responses to fraud attempts (Chen et al., 2023). However, one of the main challenges in implementing these systems is addressing ethical issues related to data privacy and algorithmic bias (Dhirani et al., 2023). AI systems require access to large amounts of personal and transactional data to function effectively, thus raising questions about how that data is collected, stored, and used. Algorithmic bias arises when models are trained on historical data that reflect social inequalities, potentially leading to disproportionate targeting of certain demographic groups and producing unfair fraud detection outcomes (Al-Dosari et al, 2024). This bias can reinforce existing inequalities, making some populations more likely to be flagged as suspicious even though their financial behavior is like that of other groups.

Furthermore, while cybersecurity is crucial in fraud detection, there is a gap in that AI-based fraud detection systems face significant security challenges. With increasing adoption, these systems have become prime targets for cybercriminals, who can carry out adversarial attacks by subtly manipulating transaction data to deceive AI algorithms and bypass detection mechanisms (Kalla & Kuraku, 2023). In addition, inversion attacks allow malicious actors to reverse engineer AI systems to gain insight into the algorithm's decision-making process, thereby threatening the integrity of the system. This vulnerability highlights the need for robust cybersecurity protocols and careful monitoring of algorithmic bias, so that AI-based fraud detection systems perform effectively (Ali et al., 2024).

Based on cases of bias in the use of AI in financial systems, it appears that the application of AI has risks that could potentially harm both consumers and financial service providers. These risks arise mainly because AI is highly dependent on data as the main source in the learning and decision-making processes. Data imbalance can cause algorithms to interpret information unfairly. Furthermore, the use of black-box algorithms poses challenges in terms of explainability and transparency. In addition, the widespread use of personal data raises ethical challenges related to privacy, security, and transparency, which require the implementation of careful data processing mechanisms, algorithm audits, and periodic fairness evaluations before and during the implementation of AI systems in the financial sector.

2.2. AI – related Regulations in Indonesia and Multiple Jurisdictions

2.2.1 Banchmarking AI Regulations and Cases in Various Jurisdictions (EU, US, China, Singapore, Australia, Qatar)

A. European Union (EU)

The European Union's AI Act (2024), effective on 1 August 2024, represents the world's first comprehensive regulatory framework for artificial intelligence, designed to balance innovation with human rights and social welfare. It introduces a risk-based classification: (1) unacceptable-risk AI, banning practices such as social scoring, predictive policing, and untargeted facial scraping, as these practices are deemed harmful or unethical and are prohibited under the Act (Novaes, R.V., & Wanderley Jr, B., 2025) (2) high-risk AI, requiring strict conformity assessments for systems affecting areas like medical treatments, employment opportunities, or loans for purchasing real

estate;[1] (3) AI with transparency obligations, covering those for direct interaction with people, generating synthetic content, emotion recognition, biometric categorization, deep fakes, and manipulating public interest-related texts; and (4) minimal-risk AI, such as spam filters and AI-powered video games,[2] subject to voluntary codes of conduct.

Although not sector-specific, the Act has significant implications for finance, particularly for institutions using high-risk AI, particularly in credit scoring and risk assessment in the case of life and health insurance, fraud monitoring, customer profiling, and product reaction, where compliance into their existing governance frameworks is a mandatory (Passador, M.L., 2024) Coordination between the European AI Office and the European Central Bank underscores its role in financial oversight,[3] ensuring AI systems align with prudential regulation, financial stability, and ethical governance.

Considering that the AI Act is in its transitional period, it is justifiable that no jurisprudence has yet referenced the AI Act as the foundation for decisions. However, generative AI raises important concerns about privacy and data protection (Claudio Novelli, et. al., 2024). In Germany, the Cayla doll was banned due to covert surveillance risks threatening children's privacy,[4] while in Italy, OpenAI was fined €15 million for unlawful personal data processing in training ChatGPT.[5] Additionally, the CJEU's *SCHUFA* ruling prohibited purely automated credit scoring, highlighting the risks of AI in sensitive contexts.[6] These cases reinforce the AI Act's necessity.

B. United States (US)

Unlike the European Union's comprehensive AI Act, the United States lacks federal legislation directly regulating AI, relying instead on executive action, sector-specific oversight, and voluntary industry commitments (self-regulation) (Davytan T, 2025). The Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (October 2023) directed over 50 agencies to address risks related to cybersecurity, privacy, consumer protection, and bias.[7] In the financial sector, initiatives such as the Treasury Report emphasize embedding AI risk management within broader frameworks, while agencies like the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and The Consumer Financial Protection Bureau (CFPB) explore AI's impact on trading, credit scoring, and consumer protection. State-level measures, notably in California, also advance AI accountability. A subsequent Executive Order (January 2025) reinforced U.S. priorities in economic competitiveness, security, and human well-being while reviewing existing regulations.[8] Overall, the U.S. employs a decentralized, market-driven model that contrasts with China's state-driven approach and the EU's rights-based framework, balancing innovation with voluntary standards and sector-specific oversight (Davytan, T., 2025)

Recent U.S. cases illustrate the complex legal challenges posed by AI. In *Turner v. Nuance* and *Gladstone v. Amazon Web Services, plaintiffs* alleged privacy violations under the California Invasion of Privacy Act, stressing that AI operators must secure explicit

---

[1] European Commission, 'Artificial Intelligence Q&As' (1 August 2024), https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683

[2] Intersoft Consulting, 'Artificial Intelligence Act - AI Act law', https://ai-act-law.eu/.

[3] European Commission, 'European AI Office', https://digital-strategy.ec.europa.eu/en/policies/ai-office

[4] European Union Agency for Fundamental Rights, European Court of Human Rights Council of Europe, and European Data Protection Supervisor, Handbook on European Data Protection Law (Publication Office of the European Union, 2018), 365.

[5] Giada Zampano, "Italy's Privacy Watchdog Fines OpenAI for ChatGPT's Violations in Collecting Users Personal Data," *Apnews*, December 20, 2024, https://apnews.com/article/italy-privacy-authority-openai-chatgpt-fine-6760575ae7a29a1dd22cc666f49e605f

[6] CJEU Case C-634/21, SCHUFA case, OQ v Land Hessen, accessed September 10, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CA0634#ntr1-C_202400913EN.000101-E0001

[7] A&O Shearman, "Zooming in on AI - #5: AI under Financial Regulations in the U.S., EU and U.K. – A Comparative Assessment of the Current State of Play: Part 1," September 23, 2024, https://www.aoshearman.com/en/insights/ao-shearman-on-tech/zooming-in-5-ai-under-financial-regulations-in-the-us-eu-and-uk-a-comparative-assessment-part-1.

[8] The White House, "Removing Barriers to American Leadership in Artificial Intelligence," *Presidential Action*, January 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

consent and comply with all applicable laws. Intellectual property issues also arise, as in *Getty Images v. Stability AI*, where Getty claims millions of copyrighted images, along with associated metadata and captions, were unlawfully used to train the generative AI of Stable Diffusion,[9] potentially infringing copyright and misusing watermarks.[10] Similarly, *Thomson Reuters v. Ross Intelligence*[11] involved unauthorized use of Westlaw headnotes; the court rejected Ross's fair use defense,[12] finding its commercial use non-transformative and harmful to the market (Ginsburg, J.C., 2020). Ethical risks are highlighted by attorney Zachariah Crabill's suspension[13] after submitting a court filing generated by ChatGPT containing fabricated citations. Collectively, these cases underscore the urgent need for robust legal frameworks addressing privacy, intellectual property, and ethical standards to ensure responsible AI integration in law and beyond.

C. Singapore

Singapore has taken a proactive role in AI governance since launching its Model AI Governance Framework in 2019 and the National AI Strategy (NAIS). These initiatives aim to promote ethical AI adoption while advancing impactful projects in healthcare, education, urban services, and border operations. NAIS is supported by five enablers: international collaboration, AI talent, data architecture, trusted environments, and public-private partnerships. A robust data governance ecosystem underpins these efforts, with frameworks such as the Data Sharing Framework and Public-Private Data Sharing Framework ensuring secure and privacy-conscious use of data.

Currently, Singapore lacks regulations that are specifically tailored to the governance of AI. Singapore is adopting a sectoral approach, rather than issuing a comprehensive AI regulation that applies to all industries. This involves the publication of guidelines and regulations by individual ministries, authorities, and commissions. For example, in the financial sector, the Monetary Authority of Singapore (MAS) introduced the FEAT principles (Fairness, Ethics, Accountability, Transparency) and the Veritas initiative[14] to operationalize them in banking (customer marketing and credit risk scoring) and insurance (insurance predictive underwriting, customer marketing, and insurance fraud detection). In December 2024, MAS further issued AI Model Risk Management Guidelines, mandating (1) oversight and governance of AI, (2) key risk management systems and processes for AI, and (3) development, validation, and deployment of AI.[15]

The case of *Quoine Pte Ltd v B2C2 Ltd* illustrates how courts address contractual disputes involving deterministic algorithms.[16] Here, cryptocurrency trades executed at abnormal prices due to platform glitches were later cancelled by Quoine. The court held the transactions valid, emphasizing B2C2's good faith and Quoine's lack of justification for unilateral cancellation. However, this reasoning may not extend to AI systems capable of machine learning, which adapt their decision-making beyond programmer intent. This raises accountability questions—whether liability lies with programmers, users, or both. In Singapore, negligence law is fault-based, requiring proof of duty of care, breach, and

---

[9]Blake Brittain, "Getty Images lawsuit says Stability AI misused photos to train AI," *Reuters*, February 6, 2023, https://www.reuters.com/legal/getty-images-lawsuit-says-stability-ai-misused-photos-train-ai-2023-02-06/.

[10] Case 1:23-cv-00135-UNA, Demand for Jury Trial, *Getty Images vs. Stability AI, Inc.*, The United States District Court for the District of Delaware, See also Getty Images US, Inc. v. Stability AI, Inc., Case No. 66788385, *CourtListener*, https://www.courtlistener.com/docket/66788385/getty-images-us-inc-v-stability-ai-inc/.

[11] Case 1:20-cv-613-SB, Memorandum Opinion, Thomson Reuters Enterprise Centre GMBH and West Publishing Corp., p.3

[12]Case 1:20-cv-613-SB, Memorandum Opinion, Thomson Reuters Enterprise Centre GMBH and West Publishing Corp., p.3.

[13] Ishita Srivastava, "Colorado attorney is suspended from the bar and fired from his firm for using ChatGPT in court after the AI cited fake case", *Dailymail*, April 30, 2024, https://www.dailymail.co.uk/news/article-13367897/Colorado-attorney-suspended-bar-fired-chatgpt-ai.html.

[14] Monetary Authority of Singapore, *Veritas Initiative: What It Is*, October 23, 2023, https://www.mas.gov.sg/schemes-and-initiatives/veritas

[15] Monetary Authority of Singapore, *Artificial Intelligence (AI) Model Risk Management: Observations from a Thematic Review*, paras. 6.1–6.5, December 5, 2024, https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management;

[16] Quoine Pte Ltd v B2C2 Ltd (n 58). For a case commentary, see A Loke, 'Mistakes in Algorithmic Trading of Cryptocurrencies' (2020) 83 (6) Modern Law Review 1343

damage, yet software malfunctions complicate breach assessment (Chen, S., Lim, J.H.S., & Lim, B.K.L., 2020). Similarly, product liability demands evidence of defects, making claims difficult. Scholars suggest limited reforms combining negligence and product liability with no-fault features, rather than full strict liability, to balance costs and fairness. Although Singapore has no major AI misuse cases, debates on liability, data rights, and ownership remain pressing.

D. Australia

Australia has progressively advanced its AI governance framework, beginning with the AI Ethics Principles issued in 2019 by the Department of Industry, Science, and Resources (DISR) and CSIRO. These eight voluntary principles emphasize accountability, transparency, privacy, fairness, safety, and human-centered values, guiding organizations in the responsible design, development, and deployment of AI. Industries may not be required to consider all the principles if the use of AI does not involve or affect human beings.[17]

1. Establish, implement, and publish an accountability process including governance, internal capability and a strategy for regulatory compliance.
2. Establish and implement a risk management process to identify and mitigate risks.
3. Protect AI systems, and implement data governance measures to manage data quality and provenance.
4. Test AI models and systems to evaluate model performance and monitor the system once deployed.
5. Enable human control or intervention in an AI system to achieve meaningful human oversight.
6. Inform end-users regarding AI-enabled decisions, interactions with AI and AI-generated content.
7. Establish processes for people impacted by AI systems to challenge use or outcomes.
8. Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks.
9. Keep and maintain records to allow third parties to assess compliance with guardrails.
10. Engage your stakeholders and evaluate their needs and circumstances, with a focus on safety, diversity, inclusion and fairness.

Figure 1 The 10th Voluntary AI Safety Standard Australia

In June 2024, the government introduced the National Framework for AI Assurance, which sets standards for AI use in the public sector, focusing on lawful application, risk mitigation, and demonstrable safety. Complementing this, the National AI Centre released the Voluntary AI Safety Standard in August 2024, establishing ten guardrails across the AI supply chain, with proposals for mandatory adoption in high-risk contexts, as in Figure 1.[18] These preventative measures necessitate that developers and deployers of AI in high-risk environments implement actions to guarantee the safety of their products.

At the state level, New South Wales (NSW) enforces its own AI Assurance Framework[19], mandating oversight, risk assessment, and adherence to ethical principles. Internationally, Australia aligns with OECD, Bletchley, and Seoul Declarations, while considering risk-based legislation targeting high-risk AI models. The government is contemplating the implementation of a risk-based regulatory approach, which would prioritize high-risk AI applications while permitting low-risk applications to thrive, by applying mandatory guardrails by the following options: 1) integrating them into existing regulatory frameworks; 2) enacting framework legislation with corresponding revisions to current laws; or 3) establishing a new cross-economy AI Act. Meanwhile, the Australian Securities and Investments Commission (ASIC), stressed that AI use must align with

[17]Department of Industry, Science and Resources (Australia), "Australia's AI Ethics Principles," *Australia's Artificial Intelligence Ethics Principles*, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles.

[18] Department of Industry, Science and Resources, *Voluntary AI Safety Standard* (Canberra: Commonwealth of Australia, 2024), https://www.industry.gov.au/sites/default/files/2024-09/voluntary-ai-safety-standard.pdf, v-vii.

[19] NSW Government, "NSW Artificial Intelligence Assessment Framework", 2024, https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assessment-framework.

existing obligations—fairness, transparency, avoidance of exploitation, and directors' duties of care.[20]

In parallel, the government is reviewing the Australian Consumer Law to clarify its applicability to AI-enabled goods and services and ensure remedies for harm. The *Robodebt* scandal highlights the dangers of poorly designed automated systems to determine indebtedness, which caused severe social and legal harm[21] through unlawful data-matching practices. In intellectual property law, the *DABUS* case marked a turning point: the Federal Court recognized AI as an inventor under the Patents Act, [22] though only humans or legal persons may hold patent rights.

E. China

China has adopted a proactive regulatory approach to generative artificial intelligence (AI), emphasizing both technological progress and national security. In July 2023, it enacted the Interim Measures for the Management of Generative AI Services, the world's first legally binding framework specifically targeting generative AI. The Measures impose strict obligations on providers, including compliance with data security laws, content filtering, algorithm registration, and labeling of AI-generated outputs (Zou & Zhang, 2025). Providers are treated as content producers and held liable for AI-generated material - a stance criticized for imposing disproportionate responsibility without clarifying users' obligations. Unlike the European Union's AI Act, which applies horizontally to all AI systems, China adopts a vertical model focused on specific technologies and their risks, particularly content security and misinformation prevention. The September 2024 content-labeling regulation further reinforces state oversight. Overall, China's governance model reflects a security-oriented, state-driven approach to AI, contrasting with the market and rights-based frameworks of the US and EU.

China has rapidly integrated AI into financial markets, particularly in quantitative and high-frequency trading, but this has raised risks of manipulation and instability. In 2023, the CSRC investigated a hedge fund for AI-driven "spoofing," [23] part of 64 manipulation cases recorded (Zulkifley et al., 2023) To address such risks, the 2023 Securities Law and CSRC Algorithmic Trading Regulations mandate AI model registration, risk controls, disclosure, and real-time monitoring.[24] Beyond trading, the CSRC combats AI-driven misinformation with stricter oversight, proactive rumor clarification, and investor education. Complementary laws, including the Personal Information Protection Law (PIPL) and Interim Measures on Generative AI, emphasize transparency, liability, and consumer protection.

F. Qatar

The Qatar Central Bank (QCB) issued its AI Guidelines 2024, [25] effective from September 4, 2024, to promote the safe, transparent, and accountable use of AI in the financial sector. The guidelines define AI as technologies simulating human traits such as reasoning, problem-solving, learning, and planning, and apply to entities that develop, acquire, or outsource AI systems. Unlike the EU AI Act, the QCB framework is non-binding and does not prescribe sanctions for misuse. Structured into six parts and

---

[20] ASIC, "Beware the gap: Governance arrangements in the face of AI innovation", October 29, 2024, https://www.asic.gov.au/regulatory-resources/find-a-document/reports/rep-798-beware-the-gap-governance-arrangements-in-the-face-of-ai-innovation/.

[21] Australian Government, "Robodebt class action", last modified September 4, 2025, https://www.servicesaustralia.gov.au/robodebt-class-action?context=6027.

[22] *Thaler v Commissioner* of Patents [2021] FCA 879, see: https://haugpartners.com/wp-content/uploads/2021/12/Australia-Thaler-v-Commissioner-2021-FCA-879.pdf.

[23] Reuters, "China to Crack Down on Stock Market Fake News as AI Spurs Misinformation," *Reuters*, March 15, 2025, https://www.reuters.com/world/china/china-crack-down-stock-market-fake-news-ai-spurs-misinformation-says-state-media-2025-03-15/.

[24] Jushan Wang & Kexiao Sun, "Legal Update: AI Regulations and Compliance," *Lexology*, April 24, 2024, https://www.lexology.com/library/detail.aspx?g=0f1fafca-3fab-4b08-baed-8c28e086f09d.

[25] Martin Hayward, "Qatar Central Bank Guidelines on Ethical AI in the Financial Sector," *Pinsent Masons*, September 26, 2024, https://www.pinsentmasons.com/out-law/news/qatar-central-bank-guidelines-ethical--ai-financial-sector.

twenty-four sub-chapters, the guidelines emphasize governance, human oversight, life cycle management, customer protection, and compliance with secondary regulations. Key obligations include adopting an AI strategy, establishing oversight mechanisms, and maintaining a registry of AI systems. Financial institutions are also required to submit regular reports to the QCB, covering risk assessments, impact analyses, and technical details. Overall, the guidelines provide a principle-based framework balancing innovation with risk management in Qatar's financial sector.

Qatar lacks AI specific legislation for the financial sector, but oversight falls under the Qatar Central Bank Law No. (13) of 2012, which grants the QCB broad regulatory and supervisory powers. The law established the Financial Stability and Risk Control Commite and tasked the QCB with ensuring financial stability, consumer

Qatar lacks AI-specific legislation for the financial sector, but oversight falls under the Qatar Central Bank Law No. (13) of 2012, which grants the QCB broad regulatory and supervisory powers. The law established the Financial Stability and Risk Control Committee and tasked the QCB with ensuring financial stability, consumer protection, and market integrity. Financial institutions remain fully accountable for violations arising from human error or AI systems, with obligations to investigate breaches and report them to the QCB. Enforcement measures may include warnings, directives, monetary sanctions, or license revocation. Additionally, Qatar's Personal Data Protection Law applies, given AI's reliance on processing sensitive personal data in financial services.

G. Indonesia

Indonesia's AI regulation in the financial sector remains fragmented across multiple institutions. BI [26] and OJK [27] focus on innovation oversight, consumer protection, and ethical fintech practices, while the Ministry of Communication and Digital[28] promotes a holistic national framework grounded in ethics, transparency, and security. Law No. 1, 2024 on the Amendment of the Electronic Information and Transactions (EIT Law)[29] and Law No. 17/2022 on Data Protection Law (PDP Law) provide the statutory foundation for accountability and data protection. While the financial sector is not yet prioritized in Indonesia's AI national strategy, regulatory sandboxes and ethical guidelines suggest a gradual shift toward a more comprehensive liability and governance model. To remain aligned with international standards, Indonesia must consolidate its dispersed frameworks into a cohesive legal regime that ensures innovation is balanced with fairness, consumer rights, and systemic stability.

2.3. The Regime Liability Framework

2.3.1 Identification of Legal Subject in AI

Globally, AI is treated as an object of regulation, not a legal subject. The EU's AI Act explicitly confirms that liability for harm rests with human actors, not AI itself.[30] Courts, such as in *Thaler v. Comptroller General of Patents* (UK), have similarly ruled that inventorship requires a human, rejecting AI as a rights-holder. In Indonesia, legal subjects are limited to natural persons and legal entities. While no law explicitly governs AI, the amended ITE Law 2024 regulates "electronic agents," whose actions are legally attributed to their providers. Thus, responsibility for AI's conduct rests with system organizers under UU ITE and PP 71/2019. Obligations include data confidentiality, privacy, and transparency safeguards. Indonesian scholarship stresses that AI cannot independently commit unlawful acts; liability must be traced to developers, deployers, or controllers. Although some theorists propose extending legal personhood to AI,

[26] Bank Indonesia (BI) Regulation No. 22/23/PBI/2020, No. 23/6/PBI/2021, No. 3/PBI/2023
[27] OJK, *Code of Ethics for Responsible and Trusted AI.*
[28] Regulation Number 3 of 2021
[29] Article 1 point 8 Electronic System
[30] Article 57(12) e final European AI Act.

Indonesian law has not recognized such standing, reaffirming AI's status as a tool under human accountability (Kurniawan,I.D., & Kristayadi., 2022).

2.3.2 The Theory of Liability Framework in Consumer Protection

AI cannot be held legally liable, so responsibility rests with the humans or corporations behind it. In Indonesia, liability generally follows two models: **fault-based liability** and **strict liability** (Singh, M., 2020). In many developing jurisdictions, fault-based liability still dominates due to its perceived fairness and protection of business interests. However, critics argue it imposes a heavy burden on consumers who may lack the resources or technical knowledge to demonstrate fault effectively. Modern products often involve complex manufacturing chains, making it difficult for consumers to access evidence of negligence (Singh, M., 2020) Moreover, fault-based liability is less effective in regulating industries where risks are not easily attributable to human error. Fault-based liability, grounded in Article 1365 of Indonesian Civil Act (KUHPerdata) and Article 19 of the Consumer Protection Law (UUPK), requires proof of negligence, causation, and damage, but this often burdens consumers who lack resources to establish fault, which aligns with (Hamzah, A. & Rachmawati, I.,2022). The concept of fault-based liability also applies in Article 42 sections (1) and (2) of Bank Indonesia Regulation on Consumer Protection, as well as in Article 236 section (2) of the Law on the Development and Strengthening of the Financial Sector (P2SK Law).

Strict liability is based on the rationale that those who profit from selling goods should also bear the risk of defects, given their control over production and safety standards (Choi, S. & Kim, D., 2019). Legal scholars have emphasized that strict liability serves both compensatory and preventive functions, as it incentivizes producers to improve safety standards while ensuring fair compensation for consumers (Owen, D.G., 2019). Consumers harmed by defective products often face difficulty identifying who was negligent. Was it the designer, the coder of embedded software, or the final distributor? This legal fog makes fault-based litigation nearly impossible. Strict liability cuts through this complexity by allowing consumers to sue any party in the chain of distribution, with the assumption that those actors can sort liability among themselves through indemnification. In the EU and several ASEAN countries, strict liability is also applied to non-physical products like digital content and software, reflecting the digitization of modern consumption (OECD, 2023).

Article 8(2) of the Consumer Protection Law prohibits selling defective or used goods without full disclosure, while Article 19 obligates businesses to compensate consumers for harm caused by their products or services under strict liability. However, liability may be waived if the business proves the consumer was at fault. The application of strict liability regime in Indonesia under this law remains limited. Both models highlight the need to balance innovation, accountability, and consumer protection in AI-related harms.

3. Methodology

3.1 Normative Juridical Approach

This study employs a juridical-normative research method, which is a legal research approach based on the examination of legal materials such as legislation, jurisprudence, and legal doctrines. The purpose of this method is to analyze legal issues normatively—by relying on written and prevailing legal norms. In this context, various laws and regulations, court decisions (jurisprudence), and scholarly legal opinions (doctrines) related to AI are used to examine and analyze the legal issues arising from the development and application of AI technologies.

By using this approach, the research focuses on how existing positive law regulates, responds to, or has yet to address the legal challenges posed by AI, such as legal liability, data protection, and ethical implications. Through the juridical-normative method, this study aims to provide a comprehensive understanding of the adequacy and effectiveness

of the current legal framework and offer critical analysis on the need for legal reform in anticipating future developments in AI technology.

3.2 Comparative Juridical Approach

The methodology of comparative law involves a structured process comprising four steps: developing comparative skills, evaluating external laws, evaluating internal laws, and making comparative observations to systematically analyze legal systems.[31] This approach promotes rigorous legal comparison to gain broader insights into diverse legal traditions and their relevance to global legal challenges.[32]

Based on this methodology, this research compares relevant laws on AI in the financial sector from Indonesia (internal law) and jurisdictions outside Indonesia, including the European Union, the United States, China, Singapore, Australia, and Qatar (external law), and examine how these regulations are implemented in each country. In addition, the study assesses the adequacy of Indonesia's regulatory framework on AI in the financial sector as well as evaluate the sufficiency of the liability framework for consumer protection in this sector. Ultimately, this research aims to propose a regulatory framework for the use of AI in the financial sector and a liability framework for consumer protection in the financial sector for Indonesia.

3.3 Empirical Juridical Approach

Juridical-empirical research methodology collects factual data from society to examine how law works in practice. It combines legal analysis with real-world data and facts to measure the effectiveness of a legal arrangement. The data collection techniques include observation, interviews, surveys, and case studies.[33]

This study conducted a focus group discussion with four key industry players : Bank Mandiri, GoTo Financial, Dana, and Superbank to explore the application of artificial intelligence in financial services and its consumer protection implications. Key discussion points included AI integration in business processes, challenges related to consumer protection, compliance with transparency and fairness principles, handling consumer complaints from AI decisions, and future AI development plans aimed at improving services while prioritizing consumer protection. The discussion is summarized in the appendix of this paper.

4. Results / Analysis

4.1. Regulatory Framwork of AI in finansial sector

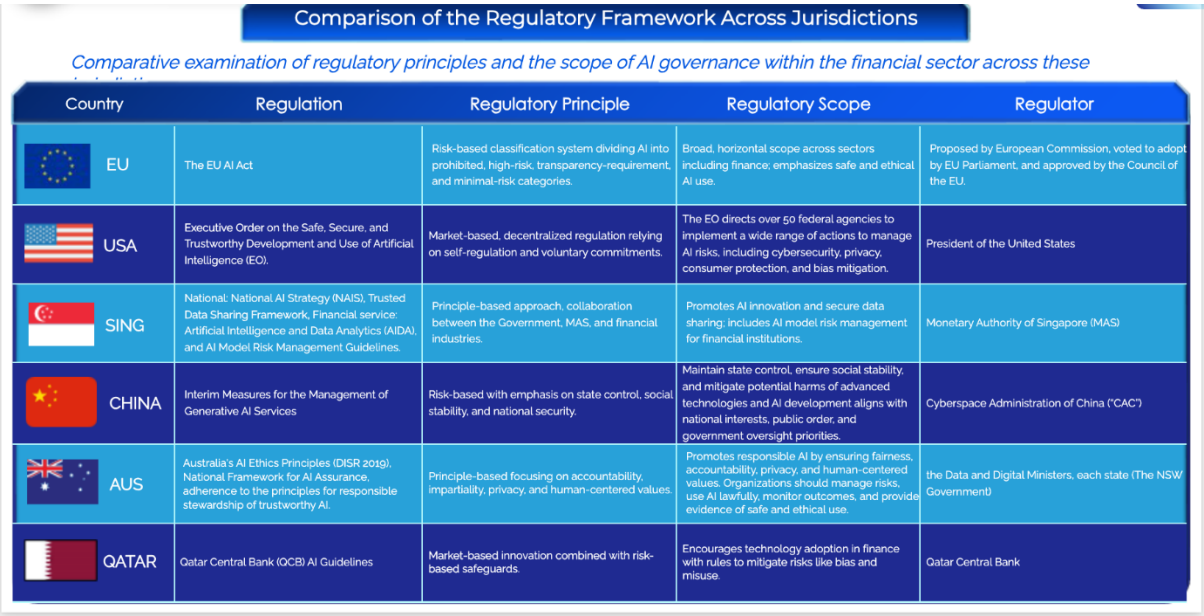
4.1.1 Global Regulatory Framework of AI in Finansial Sector

Building on the cross-jurisdictional analysis of AI implementation across various legal systems presented in the previous chapter, this section evaluates the adequacy of current regulatory frameworks governing AI applications in the financial sector, highlighting key challenges and potential directions for future development. Globally, the regulation of Artificial Intelligence (AI) reflects a wide spectrum of approaches—from comprehensive legislative instruments, such as the EU's AI Act, to sector-specific ethical guidelines and standards observed in countries like the United States, Singapore, and Australia. The prevailing trend suggests a continued expansion and growing complexity of AI regulations in the years ahead.

To further elucidate these diverse regulatory strategies and deepen the analysis, a comparative examination of regulatory principles and the scope of AI governance within the financial sector across these jurisdictions is provided in the table below.

---

[31] Edward J. Eberle, "The Methodology of Comparative Law, *Roger Williams University Law Review* 16, no. 1 (2011), 72-23.
[32] *Ibid.*
[33] Adco Law, "Legal Research Methods in Legal Problem Solving," *Adco Law*, March 7, 2022, https://adcolaw.com/blog/legal-research-methods-in-legal-problem-solving/.



Country	Regulation	Regulatory Principle	Regulatory Scope	Regulator
EU	The EU AI Act	Risk-based classification system dividing AI into prohibited, high-risk, transparency-requirement, and minimal-risk categories.	Broad, horizontal scope across sectors including finance; emphasizes safe and ethical AI use.	Proposed by European Commission, voted to adopt by EU Parliament, and approved by the Council of the EU.
USA	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO).	Market-based, decentralized regulation relying on self-regulation and voluntary commitments.	The EO directs over 50 federal agencies to implement a wide range of actions to manage AI risks, including cybersecurity, privacy, consumer protection, and bias mitigation.	President of the United States
SING	National: National AI Strategy (NAIS), Trusted Data Sharing Framework, Financial service: Artificial Intelligence and Data Analytics (AIDA), and AI Model Risk Management Guidelines.	Principle-based approach, collaboration between the Government, MAS, and financial industries.	Promotes AI innovation and secure data sharing; includes AI model risk management for financial institutions.	Monetary Authority of Singapore (MAS)
CHINA	Interim Measures for the Management of Generative AI Services	Risk-based with emphasis on state control, social stability, and national security.	Maintain state control, ensure social stability, and mitigate potential harms of advanced technologies and AI development aligns with national interests, public order, and government oversight priorities.	Cyberspace Administration of China ("CAC")
AUS	Australia's AI Ethics Principles (DISR 2019), National Framework for AI Assurance, adherence to the principles for responsible stewardship of trustworthy AI.	Principle-based focusing on accountability, impartiality, privacy, and human-centered values.	Promotes responsible AI by ensuring fairness, accountability, privacy, and human-centered values. Organizations should manage risks, use AI lawfully, monitor outcomes, and provide evidence of safe and ethical use.	the Data and Digital Ministers, each state (The NSW Government)
QATAR	Qatar Central Bank (QCB) AI Guidelines	Market-based innovation combined with risk-based safeguards.	Encourages technology adoption in finance with rules to mitigate risks like bias and misuse.	Qatar Central Bank

Figure 2 Comparison of the Regulatory Framework Across Jurisdictions

This comparison details key characteristics such as the legal basis, regulatory principles, scope, and responsible authorities, thereby offering a structured overview of how each jurisdiction addresses the challenges posed by AI deployment in finance. By juxtaposing these elements, the table clarifies areas of regulatory convergence and divergence, which is critical for assessing global coherence in AI governance and identifying best practices to inform future regulatory developments.

Furthermore, regarding the proposed appropriate regulatory framework for the use of AI in the financial sector, based on the comparative regulatory tables presented, this paper formulates a typology of regulatory approaches that may be adopted by national jurisdictions in response to the evolving deployment of AI within the financial sector. These approaches are not prescriptive but are designed to be adaptable to the unique characteristics of each country's legal tradition (e.g., civil law, common law, or hybrid systems), the institutional strength and objective of its regulatory authorities, and the maturity level of AI adoption in its financial services industry. The typology accounts for both doctrinal underpinnings and practical governance challenges, recognizing that jurisdictions may pursue diverse objectives—such as fostering innovation, ensuring consumer protection, preserving financial stability, or asserting sovereign control over digital infrastructures. As such, the regulatory models identified herein are intended to serve as strategic frameworks that policymakers can calibrate or combine to suit their specific legal, economic, and technological contexts.

1. Comprehensive Precautionary Risk-Based Statutory Model

A comprehensive, rules-based regulatory framework established through legislation that categorically governs AI for use in financial services based on risk tiers. This model embeds the precautionary principle – regulators set ex ante requirements (e.g. transparency, human oversight, risk controls) proportionate to an AI system's risk level – and enforces them through binding law. It treats high-risk AI applications (such as credit scoring or fraud detection) as subject to stringent obligations, often including pre-deployment conformity assessments or licensing, while lower risk uses face lighter rules. The doctrine is characterized by codified definitions and prohibitions (e.g. bans on AI that undermine fundamental rights), providing clear legal standards and enforcement of powers from the outset. The doctrine is characterized by codified definitions and prohibitions (e.g. bans on AI that undermine fundamental rights), providing clear legal standards and enforcement of powers from the outset.

This model prioritizes consumer and investor protection, market integrity, and the safeguarding of fundamental rights and fairness over unchecked innovation. Its aim is to preempt harm by ensuring "trustworthy AI" in finance through strict compliance mechanisms. By imposing legal certainty and accountability on AI developers and users, it seeks to prevent discriminatory or unsafe AI outcomes and maintain public trust in financial markets.

This approach suits jurisdictions with a civil law tradition or strong regulatory state of inclination, where legislatures readily enact detailed codes for new technologies. It thrives where regulatory institutions have a high capacity to enforce complex rules, and where the financial sector's historical conduct justifies vigilant oversight (e.g. jurisdictions wary of past mis-selling scandals or systemic risks). Nations with advanced AI adoption in finance and a precautionary regulatory culture often embrace this model. Exemplary jurisdictions include the European Union, whose proposed AI Act employs a sweeping risk-based statutory scheme setting out global benchmarks.

2. Sector-Focused Principles-Based Co-Regulatory Model

A principles-based governance framework that relies on soft law instruments (guidelines, ethical principles, industry codes of conduct) rather than detailed statutes, implemented via a cooperative approach between regulators and industry. This model articulates high-level doctrinal principles – such as fairness, accountability, transparency, and privacy – as normative guidelines for AI in finance, often grounded in international standards (e.g. OECD or ISO principles). Regulatory agencies use their supervisory authority to embed these principles into existing financial regulations and expect financial institutions to internalize them, but specific compliance measures are left flexible and adaptive. Rather than prescriptive rules, regulators issue interpretative guidance and expect self-regulation or co-regulation: firms are encouraged to develop internal governance frameworks and best practices aligning with the stated principles, sometimes under the oversight of industry associations or sandboxes. Enforcement is typically ex post (after-the-fact, via existing laws on consumer protection, anti-discrimination, etc.), with regulators intervening case-by-case if AI use leads to outcomes that violate broadly applicable laws or the articulated principles. This doctrinal stance reflects regulatory agility, adjusting guidelines as AI technology evolves, instead of locking in rigid requirements prematurely.

The primary objectives are technological innovation and agility alongside basic ethical safeguards. By foregoing onerous ex ante rules, this model aims to foster innovation in AI and fintech – it assumes that a lighter touch will avoid stifling beneficial AI applications in finance. Normatively, it seeks to cultivate a culture of responsible AI through awareness and voluntary compliance, emphasizing capacity-building within firms (e.g. improving AI risk management and bias mitigation practices) over punitive measures. It also pursues regulatory learnings: by observing how principles are implemented, regulators can identify where future tighter rules might or might not be needed. Consumer protection and fairness remain goals, but these are to be achieved through flexible means (encouraging firms to uphold fairness, transparency, etc.) rather than through detailed mandates. In essence, the model strives for a balance between innovation and oversight – protecting consumers and financial stability without imposing disproportionate costs on industry during AI's nascent stages.

This approach is best suited to common law jurisdictions or those with mature financial markets that have historically favored flexible, adaptive regulation. In countries where regulators traditionally set out broad outcomes and rely on industry expertise to fill in the practice (often the case in common law systems), a principles-based model aligns with legal culture. It requires strong regulatory institutions and industry trust, as much of the burden is on financial firms to self-govern under supervisory guidance. High-capacity regulators who can monitor compliance informally (through guidance, moral suasion, supervisory reviews) are crucial. Jurisdictions with high AI adoption in finance but a policy preference for market-driven growth often adopt this model.

Examples include the United Kingdom, which has eschewed a single AI law in favor of sector-specific regulators applying cross-sector AI principles from a 2023 policy white paper. The United States likewise has taken a principles-first route at the federal level – rather than new AI laws, agencies like the FTC, CFPB, and bank regulators issue guidance on using AI in lending or trading under existing laws (e.g. fair lending statutes), and the White House has published AI Bill of Rights and executive orders as non-binding policy signals. Singapore is a leading example: the Monetary Authority of Singapore's FEAT principles (Fairness, Ethics, Accountability, Transparency) guide AI and data analytics in finance as voluntary standards, supported by toolkits (e.g. MAS's Veritas initiative) and close regulator-industry collaboration instead of formal regulation. Australia has similarly adopted AI ethics guidelines for finance without immediate legislation, reflecting its common-law, innovation-friendly stance. This model is coherent with jurisdictions that historically emphasize self-regulation and common-law "reasonableness" standards, and where regulators and market participants maintain a cooperative dialogue to fine-tune AI governance over time. It works best where the regulatory capacity to supervise informally is strong and where the financial industry has a track record of compliance and engagement with voluntary codes, thereby ensuring that the absence of hard law does not become a governance vacuum.

3. Adaptive Sandbox and Innovation Facilitation Model

An experimental regulatory approach that uses regulatory sandboxes and pilot programs as core governance tools to oversee AI deployment in financial services. Rather than imposing broad rules upfront, regulators provide a controlled environment in which firms can test AI-driven financial innovations under real market conditions, subject to limited and temporary regulatory relief. The doctrine here is one of adaptive regulations or "learning-by-doing": regulators waive or tailor certain requirements for participants (e.g. capital rules, licensing norms) for a trial period while closely monitoring outcomes. Through these sandboxes, regulatory authorities gather empirical evidence on AI's risks and benefits, which then informs the gradual development of appropriate regulations or supervisory expectations. Key features of this model include iterative guidance (rules evolve after each sandbox cohort), collaborative evaluation of AI systems by regulators and developers together, and often a multi-stakeholder advisory process to update doctrinal standards as AI technology matures. In short, law and policy in this model are prototyped in parallel with technological innovation – the "rules" emerge incrementally from sandbox findings, making the governance framework highly responsive and context-specific.

The foremost goals are technological innovation, regulatory learning, and institutional capacity building. This model explicitly aims to promote innovation and competition in fintech/AI by lowering entry barriers for novel AI solutions (through temporary regulatory flexibility). It nurtures experimentation so that potentially beneficial AI applications (e.g. in credit scoring for underserved populations, RegTech compliance tools, etc.) can be developed without immediate fear of rule violations. Concurrently, it seeks to educate regulators and build capacity: as supervisors observe sandbox tests, they improve their understanding of AI systems' functioning, which enhances their ability to craft informed, effective future regulations. Another objective is proportionality – by observing real-world outcomes, regulators can calibrate any eventual rules to be neither too lax nor overly stringent. Consumer protection and risk mitigation are pursued in a targeted, evidence-based manner: during tests, safeguards (like disclosure to test participants, risk limits, human oversight requirements) are imposed case-by-case, and only if tests reveal significant risks would broad regulatory intervention be justified. Ultimately, the sandbox approach aims to align regulatory pace with innovation pace – ensuring that governance neither lags so far behind as to allow harm, nor leaps so far ahead as to choke off useful innovations.

This model is well-suited to jurisdictions with developing AI sectors or smaller markets that seek to become innovation hubs while prudently managing risks. It requires regulatory willingness to experiment and moderate regulatory capacity – the authority

must be able to oversee sandbox experiments and analyze results, even if it has not yet developed comprehensive AI rules. Jurisdictions that have a history of using sandboxes in fintech or other sectors will find it a natural extension to AI governance. Exemplar implementations span both advanced and emerging economies. In the European Union, even as a hard-law AI Act is being finalized, regulators are concurrently mandated to establish AI sandboxes in each member state to support innovation, especially for startups and SMEs, by allowing time-limited regulatory exemptions during testing. The United Arab Emirates, aiming to brand itself as a global AI innovation center, launched an AI "RegLab" in 2019 enabling companies to obtain temporary licenses to pilot AI solutions under regulatory oversight. Singapore has run AI sandbox programs (e.g. in 2023 for generative AI in finance) to identify gaps in evaluation methods and foster technical advancements, even absent any AI-specific law. In the United States, states like Utah have introduced an "AI sandbox" via legislation in 2025, allowing firms to apply for regulatory relief to test AI-driven financial products under supervision. Other states (Connecticut, Oklahoma, Texas) are considering similar sandbox bills to stimulate fintech innovation while collecting data for future regulation. This approach is also attractive to smaller jurisdictions (including some in the Midle East and Africa) that lack extensive regulatory regimes – by adopting sandbox frameworks, they can leapfrog into AI development in finance, attracting fintech investment and honing their regulatory expertise simultaneously. Suitability also depends on a jurisdiction's market conduct history: those with relatively stable markets and fewer legacy issues may be more comfortable with controlled experimentation, whereas a history of consumer abuses might make pure sandbox approaches politically harder to justify. Nonetheless, where politically feasible, the adaptive sandbox model offers a viable global route for regulators to co-create AI governance together with industry and to dynamically balance innovation with safety nets as their financial sectors digitalize.

4. Centralized Oversight and Control Model

A state-centric regulatory approach characterized by direct, centralized oversight of AI systems in finance, often including mandatory registration, licensing, or pre-approval of AI algorithms by government authorities. Under this model, regulatory doctrine treats AI in financial services as a matter of national or systemic interest, warranting close control akin to critical infrastructure. Financial regulators (or other government agencies) establish strict criteria that AI systems must meet before and during deployment – for example, requiring firms to file detailed algorithm descriptions and risk assessments with a central registry, or obtain a certificate/license for AI-driven products before they reach consumers. Ongoing compliance is ensured through active monitoring: supervisory inspections, real-time data access, and even embedding government technical interfaces for oversight of AI operations are features of this approach. The doctrinal stance is command-and-control: clear rules of permissible vs. impermissible AI behavior are set (e.g. algorithms must not threaten social order or financial stability), and the regulator can intervene or shut down AI systems that deviate from approved parameters. This model often operates via executive or administrative regulations (rather than broad parliamentary legislation), giving regulators nimbleness to update rules, but always with a top-down enforcement posture. In sum, the centralized oversight model is defined by a high degree of regulatory gatekeeping – AI innovations in finance are not assumed beneficial by default; they must earn and retain regulatory approval under close state supervision.

The core objectives are financial stability, systemic risk prevention, and alignment with public policy goals. This model seeks to eliminate or tightly control any AI-driven activities that could undermine economic stability or consumer rights. By vetting algorithms for safety, fairness, and compliance with national interests, regulators aim to preempt systemic threats (e.g. unchecked lending AI causing a credit bubble or widespread discrimination). There is a strong consumer protection element, but unlike the broad precautionary statutory model, here protection is ensured through case-by-case control and continuous monitoring rather than across-the-board legal prohibitions.

Another key objective is to uphold sovereign oversight of technology: ensuring that critical AI infrastructure in finance operates transparently under the state's purview (sometimes tied to national security or social stability concerns). In jurisdictions adopting this model, trust in AI systems is treated as a public good guaranteed by the government's watchful eye. Additionally, this approach may aim to standardize AI practices across the industry by centrally issuing guidelines or approved techniques (for example, mandating certain explainability or data governance standards in all licensed AI systems). Unlike the innovation-focused model, here technological development is encouraged only within bounds of safety and controllability – innovation is not an end in itself but is welcomed insofar as it can be achieved without sacrificing regulatory control. Indeed, proponents view this as fostering sustainable innovation: AI can flourish, but only on a leash short enough to promptly correct course if any algorithm behaves undesirably.

This model is suited to jurisdictions with a strong central regulatory authority and a legal culture of administrative control, often observed in countries that favor government-led economic management. It aligns well with civil law systems or authoritarian governance contexts where detailed regulatory edicts and top-down enforcement are the norm, and where financial regulators have an expansive mandate to intervene in markets. High-capacity oversight institutions are a prerequisite, as this model demands technical expertise and resources for continuous monitoring of AI deployments. It is most likely to emerge in jurisdictions with high AI adoption coupled with low tolerance for failure – for example, countries that have experienced past crises or misuse of fintech and therefore insist on strict scrutiny of new AI tools. China exemplifies the centralized oversight model: its regulators have introduced detailed rules targeting specific AI applications (e.g. regulations on algorithmic recommendations and generative AI) and a centralized algorithm filing system requiring companies to register and disclose their algorithms to authorities. Chinese financial regulators likewise insist that AI algorithms in banking and lending adhere to state-set fairness and transparency criteria, and they retain authority to suspend services that threaten financial order.

Comparison of the Liability Framework Across Jurisdictions

Comparative examination of regulatory principles and the scope of AI governance within the financial sector across these jurisdictions.

Country	APPLICABLE LAW	APPLICABLE FRAMEWORK	CASES	LIABILITY PARTIES
EU	• The EU AI Act • GDPR • Product Liability Directive • The General Product Safety Regulation 2023/988/EU • intellectual property laws	Product liability	Germany: OQ v. Land Hessen (Schufa case): automated credit scoring without consumer consent	AI providers
USA	• State law (IP law, privacy law) • Examples: California Invasion of Privacy Act, California Penal Code § 631(a), § 632(a), § 637(3), The Colorado Artificial Intelligence Act (CAIA)	fiduciary liability regime	Turner v. Nuance Comme'ns, Inc and Gladstone v. Amazon Web Servs., Inc.: recording&analysis of customer calls without adequate authorization)	• Particularly providers facilitating AI services/ product • Any party involved, including AI integrator
SING	• Private law, examples: the law of mistake where actual or constructive knowledge is relevant, for example, the law of negligence • Property law (transfers of property)	• Civil liability • Criminal responsibility in relation to the operation of artificial intelligence	B2C2 Ltd v Quoine Pte Ltd SGHC(I): deployment of automated and algorithmic trading system in financial market	In the common law system, a fiduciary duty can be applied to any party who has legal obligation of AI product/service which lead to consumers loss
CHINA	• Using existing law (Copyright law)	• analisis duty of care • negligence	case of copyright of Ultraman A.I: copyright claims involving ultraman franchise.	AI providers
AUS	• The Online Safety Act 2021 • Consumer Law • The Privacy 1988 • Intellectual property laws • ASIC Act • Corporations Act • Anti-discrim ination laws • Social security law • Rule of law	• negligence, • unjust enrichment	• Robodebt Class action: automatic debt collection system which caused an automated debt recovery system miscalculated debts • Theler v Commissioner of Patents	in the common law system, a fiduciary duty can be applied to any party who has legal obligation of AI product/service which lead to consumers loss

Figure 3 Comparison of the Liability Framework Across Jurisdictions

It is important to emphasize that the delineation of these four regulatory models is not intended to be rigid or mutually exclusive. Rather, these frameworks are conceptual tools that can evolve dynamically and may be applied flexibly depending on each jurisdiction's specific legal traditions, regulatory priorities, institutional capacities, and stages of AI

maturity. A country may adopt one dominant approach or implement a hybrid model that draws elements from multiple frameworks.

For example, China combines a comprehensive risk-based regulatory structure with centralized state control mechanisms. Singapore integrates principle-based governance with regulatory sandboxes to facilitate innovation while ensuring responsible AI deployment. In some instances, jurisdictions may begin with a principles-based model to encourage experimentation and later transition to a statutory risk-based regime in pursuit of greater legal certainty and enforceability. Thus, these models are best understood as adaptable regulatory orientations that can be recalibrated over time to align with evolving technological, social, and legal objectives.

4.1.2 Evaluating AI Regulations in Indonesia's Financial Sector: Insights from Global Practice

Indonesia has made notable progress in addressing AI-related risks in the financial sector through ethical guidelines and sector-specific regulations. Nevertheless, the current approach remains fragmented and lacks a coherent, risk-based framework that systematically addresses AI's unique challenges. This highlights the need to consider whether a more integrated regulatory model—horizontal, sectoral, or hybrid—would better align with Indonesia's national priorities and institutional capacity towards a greater coherence to effectively address AI's risks in finance while supporting innovation and consumer protection.

In evaluating the current framework of Indonesia's regulation governing AI, the analysis is structured as follows:

(i) Problem definition: Critical concerns such as algorithmic discrimination, opaque (black box) decision-making, and automated profiling have not been clearly framed as distinct regulatory problems that warrant targeted intervention. Although there have been no case specifically involving bias AI reported, the use case of AI in financial sector needs to be addressed according to level of risks (high risk to low risk) and potential damage for consumers (mentally/psychologically to financially damage). This step is critical to formulate a comprehensive object of AI regulation in finance.

(ii) Identification of Regulatory Options: Based on the various models discussed above, Indonesia may derive insights from the EU's AI Act, which employs a comprehensive, risk-based approach characterized by robust public engagement, data protection, and transparency, as well as from Singapore's sectoral model that prioritizes industry collaboration. Consequently, within the "regulatory options" framework, Indonesia, akin to Singapore, adopts a sectoral strategy, integrating regulatory, co-regulatory, and non-regulatory instruments, instead of enforcing a centralized, all-encompassing AI legislation.

(iii) Data collection: For the "data collection": this step is to make an appropriate rule by incorporating public engagement as a central component. Just like in the EU, Citizens are encouraged to actively participate in shaping policy priorities and levels of ambition.[34] But in Singapore, the country focuses its data collection efforts on industry collaboration, with limited involvement from the public. Singapore intensively engages with Veritas consortium, comprising MAS, SGInnovate, professional services firms, and multiple financial institutions.[35] In Indonesia public participation in making law and regulations is mandated in Indonesia's Law No. 12 of 2011 on the Formulation of Laws and Regulations (as amended by Law No. 13 of 2022), which oblige inclusive and participatory regulatory processes as a

[34] European Commission, *Better Regulation Toolbox 2030, Chapter 7: Stakeholder Consultation* (Luxembourg: Publication Office of the European Union, 2023), 490.
[35] Monetary Authority of Singapore, *Veritas Document 3A: FEAT Fairness Principles Assessment Methodology* (Singapore: Monetary Authority of Singapore, 2020), 4.

cornerstone of legitimate and transparent governance (called meaningful participation).[36]

(iv) Assessing Alternative Options and Determining Preferable Regulatory Alternatives: Building on the typology above and recognizing the importance of aligning regulatory approaches with national contexts, a risk-based regulatory framework may offer a particularly suitable and pragmatic path forward for Indonesia.

The following section explores potential regulatory design options, drawing from international best practices and adapting them to Indonesia's legal and technological landscape

4.1.3 Designing a Fit-for-Purpose AI Regulatory Approach for the Financial Sector in Indonesia

Based on the typology above and the significance of aligning regulatory approaches with national circumstances, the following section discusses why a risk-based regulatory framework may be a good fit for Indonesia. A risk-based regulatory strategy seems relevant and practicable for Indonesia given the rising integration of AI in the financial sector.

1. Rational for Risk-based Regulation

Risk-based regulation involves using structured frameworks to prioritize oversight based on risks to society, financial systems, or regulatory agencies' objectives and effectiveness.[37] In the context of Indonesia's financial sector, this approach aligns well with existing regulatory practices—such as those implemented by the Financial Services Authority (OJK) which already apply risk-based supervision in areas like banking.[38] Furthermore, Bank Indonesia mandates stringent risk management for payment system providers in executing their operations. This method also facilitates regulatory agility and reactivity, essential for controlling the intricate and dynamic characteristics of AI systems, particularly in sectors where systemic risk, consumer protection, and financial stability are critically significant.

2. Key Elements of a Risk-Based AI Regulatory Framework

A foundational component of developing a risk-based regulatory framework for artificial intelligence (AI) in Indonesia's financial sector is the systematic identification and categorization of AI-specific risks. These include most critically, algorithmic discrimination or bias, alongside opaque or "black box" decision-making, non-transparent automated profiling, systemic errors in prediction and classification, and vulnerabilities in data privacy and cybersecurity. Among these, algorithmic bias stands out as a particularly urgent concern, given its potential to entrench financial exclusion, distort credit assessments, and disproportionately impact marginalized populations. Once these risks are identified, they may be categorized into tiers—low, moderate, and high—drawing structured frameworks such as the EU AI Act. Such stratification facilitates a proportionate regulatory response, enabling more rigorous oversight of high-risk systems while supporting innovation in lower-risk areas.

An appropriate regulatory response is crucial to guarantee that requirements are aligned with the risk levels presented by various AI systems. High-risk apps, including those utilized in credit scoring or investment advice, must adhere to compulsory transparency and explainability criteria, undergo independent audits, be subjected to algorithmic bias testing, and implement systems that safeguard customers' rights to obtain comprehensible explanations. Conversely, low-risk systems may be regulated by more lenient mechanisms such as ethical principles or voluntary codes of conduct. To facilitate this risk-based methodology, regulatory resources must be strategically allocated. Regulatory bodies like OJK and Bank Indonesia should be empowered with

[36] Article 96, UU 13 Year 2022.
[37] OECD Reviews of Regulatory Reform - Risk and Regulatory Policy - Improving the governance of risk,187.
[38] General Review of Elucidation to Financial Services authority Regulation Number 18/POJK.03/2015 concerning Implementation of Risk Management for Commercial Banks.

the authority to do system audits, investigate disputes, and enforce compliance. As the development of AI technology is in its nascent phases, sanctions are not imposed. Nevertheless, authorities ought to provide feedback and issue warnings to industries as appropriate for any violations. Sanctions on AI development would hinder innovation; concurrently, the regulator's principal purpose is to cultivate industry maturity and establish market conduct for the financial sector. The framework must be adaptable.

3. Suitable Regulatory Models for Indonesia

A hybrid regulatory model offers a context-sensitive and scalable approach for governing artificial intelligence (AI) in Indonesia's financial sector. Drawing on the four regulatory typologies identified—comprehensive risk-based statutory, principles-based co-regulation, adaptive sandboxing, and centralized oversight—this model combines their strengths while addressing Indonesia's civil law foundation, regulatory capacity, and AI adoption maturity.

In the early stages, a principles-based co-regulatory approach should guide AI for use through flexible, high-level ethical standards—such as fairness, transparency, accountability, and security—grounded in national values. Regulators and industry associations can co-develop voluntary codes of conduct to foster responsible AI adoption without stifling innovation.

As technology matures, the framework should transition toward risk-based statutory oversight, classifying AI systems by risk level (low, moderate, high) to enable proportionate intervention. High-risk applications—such as those involving opaque algorithmic decision-making—should face stricter obligations like explainability, regular audits, and consumer safeguards. This mirrors the precautionary principle embedded in the EU AI Act while respecting Indonesia's preference for codified legal clarity.

To bridge this transition, regulatory sandboxes can be deployed as adaptive governance tools. These provide controlled environments for testing AI innovations under temporary regulatory relief, enabling both empirical learning and capacity-building for regulators. Insights from sandbox iterations can inform more calibrated rulemaking over time. While Indonesia may not favor full centralized control, elements of this model—such as mandatory algorithm disclosures or supervisory access for high-risk systems—can be selectively incorporated to strengthen oversight without resorting to rigid command-and-control methods. Effective implementation depends on institutional coordination and mandate of clarity. Bank Indonesia and OJK should be empowered to audit AI systems, supervise risk management practices, and coordinate enforcement actions. Cross-agency cooperation is essential to ensure coherent, efficient oversight. Consequently, this regulation of alternative results in a financial institution being overseen by numerous authorities based on its activities. Consequently, BI and OJK will integrate their supervisory frameworks to facilitate industry compliance in report submission and adherence to necessary requirements from the authorities.

Finally, inclusive stakeholder engagement will enhance transparency and legitimacy. Multi-stakeholder forums involving regulators, industry, academia, and civil society can address concerns such as algorithmic bias and ensure that regulatory responses reflect public values.[39] In terms of data collection,[40] participatory mechanisms enable the gathering of diverse insights and empirical evidence to inform risk-based AI regulation, addressing current gaps in public disclosure and impact transparency. Meanwhile, involving stakeholders in deliberative forums also supports the assessment of alternative regulatory options by incorporating a broader range of perspectives in evaluating the proportionality, feasibility, and potential unintended consequences of different policy choices.

In sum, this hybrid approach offers Indonesia a pragmatic pathway: combining the normative clarity of civil law, the flexibility of co-regulation, the empirical grounding of sandboxes, and the proportionality of risk-based oversight. By layering these elements

[39] See appendix.
[40] Global Indicators of Regulatory Governance: Worldwide Practice of Regulatory Impact Assessments, 2.

over time, Indonesia can foster responsible AI innovation in finance while safeguarding systemic integrity and consumer trust.

4.2. Designing the Liability Framework of AI in Finansial Sector

Internationally, the question of AI's legal subjectivity has been debated. In 2017, the European Parliament famously suggested exploring a "specific legal status for robots" – essentially a form of electronic personhood for the most advanced AI – so they could be held "responsible for making good any damage" in cases where their autonomous decisions cause harm. This proposal of creating "electronic persons" was met with heavy criticism from ethicists, legal experts, and the tech industry, and it has not been adopted in any binding law. The concept raised concerns that granting personhood to AI could paradoxically let the real human stakeholders off the hook (since liability might stop at the AI's assets, or lack thereof) and that it muddles the moral agency which AI does not actually possess. The more accepted view, reflected in Indonesia's stance, is that AI should remain an object regulated through the responsibilities of its human operators and owners. Indeed, the current EU approach has shifted from talk of AI personhood and toward clarifying human accountability (e.g., transparency obligations, strict liability for producers, and presumptions of fault for operators under certain conditions).

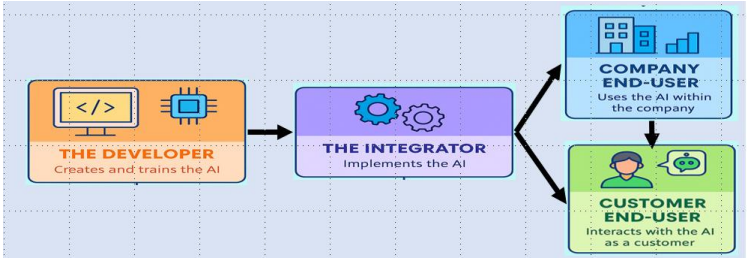


Figure 4 Interested Parties in AI

For Indonesia, maintaining AI as an electronic agent means any liability framework must identify which human or company is responsible for the AI's actions – be it the software developer, the integrator, the financial service provider deploying the AI, or potentially a data trainer or vendor.

This "attribution problem" – linking the AI's conduct to a legal subject – is central in determining liability in scenarios where something goes wrong. For instance, if a machine-learning algorithm in a peer-to-peer lending platform makes lending decisions that are deemed unlawful (perhaps discriminatory, or based on inaccurate data leading to consumer losses), who is legally answerable? Indonesian law would likely view the platform operator (the fintech company) as the "AI Operator" and thus the liable party. The Law on Electronic Information and Transaction (EIT) is expected to address that the operator of an electronic agent is responsible for its operations, except in cases of user negligence, which shifts liability to the user. Thus, Indonesian doctrine leans towards a fault-based allocation tied to control – but with elements of strict liability insofar as the operator may be liable even without personal fault, unless they can point to the user's fault.

In summary, the theoretical framework for analyzing AI liability in Indonesia combines these elements: the baseline of fault-based tort liability (negligence), potential moves toward strict liability (especially via consumer protection law for defective fintech services/products), and the rejection of AI as an independent legal actor requiring instead that a human/legal entity be found to attach liability to.

4.2.1 Model of Liability Framework Across Jurisdictions

This section analyses the approaches of different jurisdictions on accountability for injuries produced by AI, with an emphasis on consumer protection in financial services. This study evaluates frameworks within identical country groupings and examines

fundamental concepts: strict liability versus fault-based liability, the significance of legal personhood (or its absence) for AI, distribution of liability among AI supply chain participants, and mechanisms such as insurance or mandatory disclosure that support liability claims. The objective is to establish a globally suitable liability framework and subsequently determine the best appropriate model for Indonesia's consumer protection system.

It is evident that a limited number of countries have implemented formal AI legislation, as evidenced by the benchmarking of AI regulations in various jurisdictions (EU, US, Singapore, Australia, China, and Qatar). The European Union is the sole jurisdiction that regulates AI at the statutory level, out of the five that were examined. In contrast, the United States, Singapore, Australia, and China have prioritized the implementation of ethical guidelines and governance frameworks, which has provided the industry with more flexibility to innovate. It is important to note that individual state in the United States and Australia have also established their own AI governance standards.

There have been numerous legal disputes that have resulted from the implementation of AI in the financial sector. Examples include the deployment of automated and algorithmic trading systems in financial markets (Singapore: *Quoine Pte Ltd v. B2C2 Ltd*), erroneous automated debt-collection calculations (Australia), copyright claims involving the "Ultraman" franchise (China), and automated credit scoring without consumer consent (EU: *OQ v. Land Hessen*), the recording and analysis of customer calls without adequate authorization (US: *Turner v. Nuance Communications, Inc. and Gladstone v. Amazon Web Services, Inc.*). AI-related disputes have been satisfactorily resolved in the majority of cases by the existing legal frameworks and doctrines.

Fault-based liability requires the injured person to demonstrate that the defendant did not exercise due care (was negligent) or otherwise violated a duty (e.g., via recklessness or wilful misbehaviour) resulting in the harm. This is the conventional approach for services and several professional endeavours. Should an AI system's malfunction not be classified under product liability, a consumer may need to demonstrate that an individual within the development or deployment chain exhibited negligence—such as the bank's failure to properly configure or monitor the AI, or the software developer's inadequacy in testing it. Establishing negligence in AI is difficult due to algorithmic opacity and the challenge of defining a "reasonable" standard of care in the development of intricate AI systems.

Conventional legal principles—ranging from product liability to negligence—were formulated in an era characterized by human agents and physical goods. The emergence of autonomous or semi-autonomous AI contests these principles: AI judgments may lack transparency, AI software does not constitute a tangible "product" in the traditional sense, and various stakeholders (developers, integrators, users) may collectively influence an AI system's operation. In response to these challenges, some jurisdictions have adopted strict liability regimes to address disputes involving highly complex AI systems, as users are unable to comprehend the AI system’s internal functioning.

In the European Union—for example, in the Netherlands—a non-pure form of strict liability is applied in this civil-law jurisdiction, as producers or business actors must still demonstrate the existence of fault. By contrast, in common-law countries such as the United Kingdom and the United States, strict liability focuses not on fault but on the risk that causes harm. Meanwhile, Australia have implemented distinct classifications of fraud responsibilities for customers and markets. In Australia, a "point of compromise" strategy is employed to reduce disputes by attributing accountability to the entity most capable of preventing or alleviating the harm—specifically, AI developers, integrators, and/or end users. Consequently, comparing the conceptual application of strict liability across these various legal systems may inform the development of an ideal liability framework in Indonesia and strengthen legal protection for consumers.

4.3. Proposal for Conflict Resolution Caused by AI Bias

AI in financial services brings risks such as bias, opaque decisions, and data misuse, which can harm consumers and weaken trust. In Indonesia, AI-related conflicts remain limited because most financial institutions still use machine-learning tools for internal processes, and consumer-facing generative AI is still exploratory. Low public awareness also means few formal complaints. Still, preparing a conflict-resolution mechanism is urgent, given the rapid growth of AI and the absence of comprehensive regulation. A conflict-resolution framework should extend the FairSight Liability Framework by turning legal accountability into practical procedures. While FairSight clarifies who is responsible for AI harm, the conflict-resolution mechanism ensures those responsibilities can be enforced through fair, transparent, and timely processes. The proposal supports coordinated action among regulators, financial institutions, and AI developers, embedding cooperation and procedural justice into Indonesia's evolving AI governance system.

4.3.1 Collaboration between Developers and Deployers, Regulators, and Consumers

An effective conflict resolution requires an integrated approach and collaboration between related parties, namely model developers, financial institutions, regulators, and consumers who may be affected by model decisions. As AI development is progressing very fast and dynamically, it is important to involve stakeholders inclusively –regulators, industry, academia, and civil society– to establish a comprehensive AI governance framework and ecosystem. Raising awareness and understanding of risks of biases in AI to developers, users, and regulators/policymakers is essential to ensuring that mechanisms for preventing and addressing AI errors are effective and sustainable. Ethical AI principles should be adhered to ensure that the AI system of use reflects public values.

1. Developers / Deployer

As developers, the primary responsibility in AI implementation is to ensure that all AI-related regulations and principles are followed at every stage of development, from planning and design to testing and deployment. Developers should uphold the responsibility to maintain public trust in the systems they create, by addressing various critical aspects, including data transparency, system accountability, and ensuring the protection and security of consumers' personal data, as well as ethical deployment and regulatory compliance.

In this regard, transparency and explainability are central to the responsible development and deployment of AI systems and in maintaining positive relationships between developers and all stakeholders Transparency means those who deploy AI systems have a duty to clearly inform stakeholders about the presence and function of these systems and foster general awareness regarding their use. This includes disclosing its role in decision-making processes, the nature of data it processes, and its intended function. Meanwhile, explainability on the rationale behind an AI system's decision in a way that is accessible and understandable to various stakeholders, to helps them make informed decisions and fosters greater trust and accountability on the AI-powered financial services. Human review and validation (human-in-the-loop/HITL) as well as continuous active monitoring and review to ensure that the algorithmic outputs are not only technically correct but also fair and acceptable.

Developer and deployers can also work to strengthen trust in the system by highlighting the quality and reliability of the AI system, by: demonstrating the repeatability or consistent outcomes of the system the same results under identical conditions, ensuring the traceability of the AI's development, as well as facilitating auditability of the algorithm and system, which involves keeping thorough documentation of end-to-end model development process and outcomes. Information on HITL in model development is also important, to ensure accountability, ethical alignment, and trustworthiness.

Developers and deployers with hands-on experience have the deepest understanding of the latest developments and challenges in AI technology. Their practical insights are invaluable for regulators, helping shape policies and regulations that are realistic, effective, and aligned with current technical realities. By leveraging the expertise of those directly involved in AI creation and implementation, regulators can better address emerging risks and opportunities, ensuring more informed and adaptive governance frameworks.

On the dispute or conflict resolution mechanism, there should be a clear and fast channel for submitting consumer complaints, with an option to connect consumers with human representatives when needed. All complaints should be responded to promptly and transparently, followed by corrective actions when a complaint is valid.

2. Regulators

In Indonesia, regulations related to AI are still limited, both in terms of basic principles (principle-based) and specific sectoral regulations. On the one hand, existing principle-based regulations offer flexibility for sectors to tailor rules to their needs, enabling quicker adaptation to technology while ensuring safe and ethical implementation. Principle-based regulation can be challenging in practice because it requires businesses to interpret rules based on their context, leading to uncertainty and inconsistent implementation. Such limitation is reflected in the IMF AI Readiness Index 2023[41], in which Indonesia's rank was 60th. One of the four dimensions being measured is legal frameworks (Regulation and Ethics), of which Indonesia's rank was 38th.

Therefore, the role of regulators are enablers and gatekeepers, particularly to provide legal certainty while fostering an environment where AI innovation can safely transform financial services. To facilitate experimentation while enabling empirical learning and capacity building for regulators, an adaptive regulatory sandbox could be developed, such as those built in the EU, UAE, Singapore, and Utah (USA).[42] Regulators should also ensure that businesses comply with established AI principles. One way for regulators can do to ensure the compliance is through periodic audits. Regulators should also build the capacity needed to oversee and address emerging risks and adapt regulatory approaches as needed dynamically.

In addition to its regulatory and supervisory role, regulators also play a facilitative role, focusing on consumer protection and empowerment. Educating consumers about the safe and responsible use of AI technology is crucial for improving digital literacy and consumer understanding of the potential risks from the use of AI, such as potential bias in algorithmic decisions or the misuse of personal data, as well as helping them understand their rights and obligations.

Furthermore, in terms of conflict resolution, regulators must provide effective complaint channels and mechanisms for consumers experiencing issues resulting from the application of AI. Regulators play a role in ensuring that every complaint is handled thoughtfully and responsively, and that businesses are held accountable for any errors. This complaint process must include a clear and transparent resolution mechanism, allowing consumers to obtain clarity regarding the solutions provided. Thus, regulators serve not only as supervisors but also as facilitators between consumers and businesses, ensuring that AI technology is implemented in a fair, safe, and responsible manner.

3. Consumer

Consumers should play active and collaborative roles in improving their awareness and understanding of the use of AI, when and how they are interacting with AI, the potential risks they may face, as well as their rights and available protection mechanism. Consumers could also be empowered in the development of AI-based financial services, for example by involvement in pilot testing as well as providing feedback on their needs,

[41] International Monetary Fund, *AI Data Mapper* (International Monetary Fund), https://www.imf.org/external/datamapper/AI_PI@AIPI/ADVEC/EME/LIC.
[42] International Association of Privacy Professionals, "How Different Jurisdictions Approach AI Regulatory Sandboxes," *IAPP*, https://iapp.org/news/a/how-different-jurisdictions-approach-ai-regulatory-sandboxes.

experiences, and challenges when using the service. Furthermore, consumers could also promote the benefits of the services to improve acceptance and adoption by wider consumers. Should there be any AI-related complaints, consumers could first resort to AI-powered self-service dispute and resolution tools provided by the financial institution such as chatbots. Consumers should also proactively report and go through the whole resolution process should the dispute be unresolved.

4.3.2 Cross-Agency Collaboration

Collaboration and integration of the regulations between interrelated authorities play a very important role in creating a harmonious AI ecosystem and in ensuring the regulations are comprehensive, consistent, not conflicting, clear, and effective. Indonesia has various regulations to govern the use of AI, ranging from national to sectoral regulations. Those include among other are: a) Circular Letter (SE) of Minister of Communication and Informatics No. 9/2023 which outlines guidelines and ethical principles for the use and development of AI for all authorities, b) AI National Strategy (Stranas) 2020-2045 focuses on the development of economic digitalization and principle-based regulation, c) AI Code of Ethics from the Financial Services Authority (OJK) for payments, investments, insurance and online loans industry, d) Law on Electronic Information and Transactions (UU ITE), and e) Law on Personal Data Protection (UU PDP). An AI Regulatory Body could be established to harmonize the regulations across sectors and to facilitate a regulatory sandbox to foster innovation while safeguarding the consumers and meeting the standards set by regulations.

Collaboration between authorities is also needed to support an integrated and comprehensive consumer protection framework, which enables the creation of an integrated data system. This system can collect and analyze information related to violations or errors in the use of AI, allowing authorities to identify issues and provide swift and appropriate solutions. In this case, consumers who experience problems or errors in AI-based services can report the problem with clear evidence, which will be processed by the relevant authorities for corrective action. Resolving problems in the use of AI in the financial sector can also benefit from the intersectionality between authorities. Although each authority has its own problem-solving institution, collaboration between authorities allows for more holistic and effective problem handling, as well as avoids duplication of effort thus providing a more efficient solution for consumers.

On top of domestic collaboration, international collaboration on AI use in the financial sector among financial authorities is very important. It supports sharing best practices, developing common standards, managing cross-border risks, addressing ethical and regulatory challenges, and enhancing supervisory and technical capabilities.

4.3.3 Mechanism for Conflict Resolution for AI Case

The Mechanism for Conflict Resolution is suggested here as illustrated in Figure5. Conflicts can originate between customers or from AI providers. If it came from customers, it usually involves the cases of unfair treatment, bias algorithm or flawed AI that resulted in exclusion of services or ill-suited process of transactions. If it originates from an AI provider, it involves fraud attempts or executions, misuse of AI facility, or data manipulation from the customers. In this case, the complaints could also be caused by the poor design of the AI application.

When conflict occurs, the customer or AI provider, which means that the customer and AI provider could not reach an agreement following up a complaint, they should be allowed to file complaints. Authorities should provide the means to report the case as a part of consumer protection arrangement. Supervisors should do a background check to see whether the case is a legitimate case and indeed needed to be escalated to the authority. When it is legitimate and unresolved without authority intervention, the case can proceed. If not, then the supervisor should advise the complaining party that the case does not need conflict resolution by authority.

When BI receives a complaint, supervisors should then determine if the case should involve OJK as the supervisor of bank and non-bank financial institutions. If yes, then Bank Indonesia should arrange to have OJK partake in the resolutions. Supervisors should further process the case by investigating the root cause of the case by involving other related parties whenever needed. When all information is gathered, a tripartite discussion can be conducted to have an arbitration meeting. The arbitration can also be attended by another party that can help to gather further information to guarantee complete fair judgement. This other party can be an AI expert or a social service expert, or a lawyer. In this discussion, supervisors should decide if there was a violation or bias found in the AI practices, whether it came from the AI provider or the customer. If violation or bias is found, supervisor should judge according to the AI guidance or law, if it exists, whether it renders penalty or not. If yes, then a penalty is imposed. If not, the supervisor should determine if the AI provider should increase the transparency of the AI implementation by providing more explanation on how the process is conducted. If yes, then the AI provider should provide more disclosure on the AI algorithm.

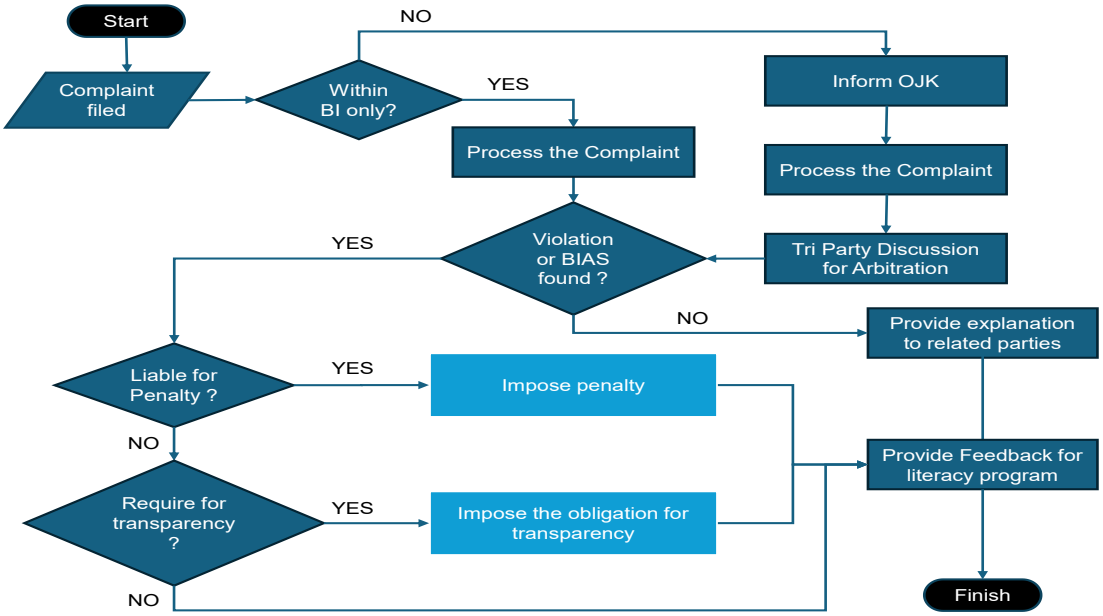


Figure 5 Conflict Resolution Flowchart

In all cases where violation of biases is found, the resolution should be fed to literacy programs. AI literacy should continuously be updated to follow the cases reported to the authorities. The arbitration meetings can also be opportunities for supervisors to update themselves on the latest development of algorithms and technology in the AI implementation. The meetings also serve as an opportunity to develop a mutual understanding between AI provider and customers to further increase the integrity of the digital financial system.

Within this arrangement, supervisors must maintain an objective and learning mode. AI may not be the supervisor's expertise. However, in the series of meetings, a supervisor needs to have an open mind and learn about the AI procedure and then use the knowledge to deliberate the best as well as the fairest decision to ensure the integrity and sustainability of AI practices. In some cases, the AI developer may have been more advanced in their implementation but forget that they must have an explainable AI (XAI) to gain customer trust in their processing of the customer's data. In this case, principle-based guidance may be beneficial to be established to support the decision-making process.

5. Implication / Policy Recommendation

5.1. Policy Recommendation

The roadmap toward a more mature AI society may still have to cover some distance for Indonesia. To bridge the current AI regulatory framework that has not addressed the liability that arises from the deployment of AI in the financial sector, this study recommends two set up: A FairSight Liability Model and A Mechanism for Conflict Resolution for AI Case.

1. A FairSight Liability Model for AI in Indonesia's Financial Services

This study argues that this liability can be workable with the current institutional arrangement of the financial authorities in Indonesia. In the previous chapter, it laid down that this liability model employs two pillars: 1) Fairness, which prioritizes consumer protection, and 2) Foresight, which ensures that stakeholders anticipate and mitigate risks before harm occurs. This approach recognizes that AI—while offering efficiency and innovation—can also produce opaque, discriminatory, or harmful outcomes if left unregulated or poorly implemented. Details of the liability model can be referred to in Part IV.2.3. of this paper.

2. A Mechanism for Conflict Resolution for AI Case

This mechanism is designed to provide a sandbox-like arrangement to resolve conflicts that may not be covered by the current regulatory framework. The case may be triggered by both consumers (e.g. potential unfair treatment, breach of data privacy) and AI providers (e.g. potential data manipulation, scam using the AI facilities). This arrangement also allows for three parties – Consumers, AI Provider, Regulators -- involved in the AI implementation to meet, learn from each other and come up with a resolution that can satisfy all parties. Within the authorities of Bank Indonesia and Indonesia Financial Service Authority, supervisory actions up to penalty to the financial institutions or escalation of the case to other authorities can be the follow up of the resolution. Details of this recommendation are covered in Part IV.3.3.

All cases covered in these two recommendations should also be fed into the AI literacy programs as lessons learned to increase the AI maturity of the financial system.

6. Conclusion and Further Research

The AI Implementation in Indonesia is underway, covering the financial system. Lots of financial institutions in the country has employed AI to provide better customer experience in the interaction with the service platforms, to support their decision-making process in customer profiling, credit assessment and product proliferation, and to empower the business process in general to stay competitive in the industry. Indonesia is a very lucrative market for AI implementation with its young and populous society is one of the darlings for big tech and financial technology in general. Several banks have transformed themselves into digital entities that already rely on AI-supported business processes to provide their edge in gaining market power. Despite all that, Indonesian customers in general have low level of digital awareness. They have yet to be sufficiently aware of the potential bias or breaches of data privacy caused by the opacity of the AI process. Discussions with the industry players confirm that there were not many major complaints caused by using AI in the financial sector. This makes Indonesia in a good position to start studying and establishing a solid AI regulatory framework. Using the methods of juridical normative, comparative and empirical, this paper collects considerations and arguments to propose using a risk-based regulatory framework to be implemented in the financial sector. This is deemed appropriate since the financial institutions have been operating and have had a lot of experience under this risk-based regulatory framework.

This paper argues that despite all the AI related laws implemented in Indonesia, algorithmic bias has not yet been systematically articulated as a regulatory issue. To effectively establish the risk-based regulatory framework for AI implementation that is ever dynamically changing, all parties involved in the industry, including the AI providers/developers, customers and authorities, must be adaptable. It suggests a roadmap to implement a hybrid regulatory model by combining comprehensive risk-based statutory oversight, principle-based co-regulation, adaptive sandboxing, and centralized oversight. The road map is as follow: 1) Early stages: a principle-based co-regulatory approach; 2) As AI implementation is growing, regulatory sandboxes can be deployed as adaptive governance tools, aimed to recommend transparency and supervisory access toward high-risk systems; 3) As technology matures: risk-based statutory oversight by classifying AI systems by risk levels (low, moderate and high) to enable proportionate intervention; 4) As the society is more matured in AI usage: a multi-stakeholder forum involving regulators, industry, academia, and civil society representing the consumers can be established to address concerns that are not yet addressed in the regulatory framework. This is to ensure that the AI regulatory framework can also evolve with technological changes. This makes Indonesia in a good position to start studying and establishing a solid AI regulatory framework. Using the methods of juridical normative, comparative and empirical, this paper collects considerations and arguments to propose using a risk-based regulatory framework to be implemented in the financial sector. This is deemed appropriate since the financial institutions have been operating and have had a lot of experience under this risk-based regulatory framework.

For the Liability Framework, this paper suggests a Clear Box Liability consisting of 1) Strict liability for high-stake use cases; 2) Rebuttable Presumptions for “Legitimate-harm” systems; 3) Use-based classification for general-purpose AI; 4) Safe harbors and Compliance incentives; and 5) Mandatory Transparency and Access Mechanism. This liability framework ensures that consumers are not borne with the impossible burden of reverse-engineering algorithms just to defend their rights. At the same time, it gives companies a clear path to manage liability by adhering to safe, auditable AI development standards.

Further study to ensure all the above frameworks are workable needs to be done collaboratively with other financial sector authorities to ensure the principle-based regulations will be inclusive for various AI implementation, oversight actions can be done in coordination across authorities when needed and every party understands each role. Increasing AI literacy to achieve mature AI society is also an important piece of endeavors that must be the responsibility of all stakeholders involved in AI implementation.

References

Adewale, G. T., Umavezi, J. U., & Olukoya, O. (2022). Innovations in Lending-Focused FinTech: Leveraging AI to Transform Credit Accessibility and Risk Assessment.

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and systems, 55(2).

Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: state-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. Mesopotamian Journal of Computer Science, 2024.

Antonevics, J. (2023). Examining algorithmic Bias in AL-Powered credit scoring: implications for stakeholders and public perception in an EU country.

Australian Government, Review of AI and the Australian Consumer Law, https://treasury.gov.au/sites/default/files/2024-10/c2024-584560-dp.pdf.

Bank Indonesia. (2020). Regulation No. 22/23/PBI/2020. Bank Indonesia.

Bank Indonesia. (2021). Regulation No. 23/6/PBI/2021. Bank Indonesia.

Beytollahi, A., & Zeinali, H. (2020). Comparing prediction power of artificial neural networks compound models in predicting credit default swap prices through Black–Scholes–Merton model. Interdisciplinary Journal of Management Studies (Formerly known as Iranian Journal of Management Studies), 13(1).

Bhatore, S., Mohan, L., & Reddy, Y. R. (2020). Machine learning techniques for credit risk evaluation: a systematic literature review. Journal of Banking and Financial Technology, 4(1).

Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. Journal of business research, 131.

Chen, S., Lim, J. H. S., & Lim, B. K. L. (2020). Attribution of civil liability for accidents involving automated cars.

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications. Data Science and Management.

Choi, S. & Kim, D. (2019). Strict Product Liability and Innovation: Evidence from Korean Manufacturing. Law and Policy, 41(3).

Davtyan, T. (2025). The us approach to ai regulation: federal laws, policies, and strategies explained. Journal of Law, Technology, & the Internet, 16(2).

Department of Industry, Science and Resources (Australia), "Australia's AI Ethics Principles," Australia's Artificial Intelligence Ethics Principles, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles.

Department of Industry, Science and Resources. (2024.). Safe and responsible AI in Australia. https://storage.googleapis.com/converlens-au-industry/industry/p/prj2f6f02ebfe6a8190c7bdc/page/proposals_paper_for_introducing_mandatory_guardrails_for_ai_in_high_risk_settings.pdf

Department of Industry, Science and Resources. (2024). Voluntary AI safety standard. Commonwealth of Australia. https://www.industry.gov.au/sites/default/files/2024-09/voluntary-ai-safety-standard.pdf.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors, 23(3).

Eberle, E. J. (2011). The methodology of comparative law. Roger Williams UL Rev., 16.

European Commission. (2023). BRT 2023 - Chapter 7: Stakeholder consultation (p. 490). https://commission.europa.eu/system/files/2023-09/BRT-2023-Chapter%207-Stakeholder%20consultation_0.pdf.

European Commission. (2024). AI Act enters into force. European Commission. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en.

European Union. (2021). Artificial Intelligence Act. European Union. https://ai-act-law.eu/.

European Union. (2023). Artificial Intelligence Act. European Union. https://ai-act-law.eu/ .

Financial Services Authority (2022) Tata Kelola Kecerdasan Artifisial Perbankan Indonesia.

Financial Services Authority. (2016). Financial Services Authority Regulation No. 18/POJK.03/2016 on the Implementation of Insurance Business.

Financial Services Authority. (2023). Code of ethics for responsible and trusted AI. Financial Services Authority. https://ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/Panduan-Kode-Etik-Kecerdasan-Buatan-AI-yang-Bertanggung-Jawab-dan-Terpercaya-di-Industri-Teknologi-Finansial.aspx.

Government of the Republic of Indonesia. (2008). Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE). Government of the Republic of Indonesia.

Hamzah, A. & Rachmawati, I. (2022). Consumer Protection in Indonesia: Between Law and Enforcement. Indonesian Journal of Consumer Law, 4(1).

Herrmann, H., & Masawi, B. (2022). Three and a half decades of artificial intelligence in banking, financial services, and insurance: A systematic evolutionary review. Strategic Change, 31(6).

Howells, G. (2021). Product Liability and Consumer Safety: The Evolution of Modern Protection. Consumer Law Review, 44(1).

International Association of Privacy Professionals. (n.d.). How different jurisdictions approach AI regulatory sandboxes. IAPP. https://iapp.org/news/a/how-different-jurisdictions-approach-ai-regulatory-sandboxes.

International Monetary Fund. (n.d.). AI Data Mapper. International Monetary Fund. https://www.imf.org/external/datamapper/AI_PI@AIPI/ADVEC/EME/LIC.

Joshua D. Greene, Sylvia A. Morelli, Kelly Lowenberg, Leigh E. Nystrom, Jonathan D. Cohen (2008), “Cognitive load selectively interferes with utilitarian moral judgment,” Cognition Volume 107, Issue 3, June 2008.

Kalla, D., Kuraku, S., & Samaah, F. (2023). Advantages, disadvantages and risks associated with ChatGPT and AI on cybersecurity. Journal of Emerging Technologies and Innovative Research, 10(10).

Kurniawan, I. D., & Kristiyadi. (2022). Questioning the existence of artificial intelligence as a legal subject in Indonesian national law. Jurnal Kewarganegaraan, 6(4), ISSN: 1978-0184, E-ISSN: 2723-2328.

Ministry of Communication and Informatics. (2021). Regulation Number 3 of 2021. Ministry of Communication and Informatics.

Monetary Authority of Singapore. (2024, December 5). Artificial intelligence (AI) model risk management: Observations from a thematic review. https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management.

Novaes, R. V., & Wanderley Jr, B. (2025). Contrasting Approaches to AI Regulation-A Comparative Analysis of the EU AI Act and China's Cyberspace Administration Decrees. Beijing L. Rev., 16.

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. Computer Law & Security Review, 55, 106066.

OECD (2010), Risk and Regulatory Policy: Improving the Governance of Risk, OECD Reviews of Regulatory Reform, OECD Publishing, Paris, https://doi.org/10.1787/9789264082939-en.

OECD. (2023). Consumer Product Safety in the Digital Age.

Owen, D.G. (2019). The Evolution of Product Liability Law: A Comparative Perspective. Journal of Tort Law, 12(2).

Passador, M. L. (2024). AI Act and the ECB: Steering Financial Supervision in the EU. Colum. J. Eur. L., 30.

Qatar Central Bank. Guidance on enforcement for financial institutions. https://www.qcb.gov.qa/PublicationFiles/Instructions_Applying_Penalties_Financial_Institutions.pdf.

Safe, S. (2023). Trustworthy Development and Use of Artificial Intelligence. The White House, Executive Order, 14110.

Singh, M. (2020). Consumer protection and the evolution of liability doctrines: A developing country perspective. Journal of Consumer Law, 23(1). https://sialim.radenfatah.ac.id/storage/GAL_11.4_1_THE%20LAW%20OF%20STRICT%20LIABILITY%20FOR%20PRODUCES%20IN%20INDONESIA.pdf.

Singh, M. (2020). Consumer Protection and the Evolution of Liability Doctrines: A Developing Country Perspective. Journal of Consumer Law, 23(1).

Smart Nation Singapore. (2019). National artificial intelligence strategy. https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf.

Thaler v Commissioner of Patents [2021] FCA 879. (2021). https://haugpartners.com/wp-content/uploads/2021/12/Australia-Thaler-v-Commissioner-2021-FCA-879.pdf.

Zampano, G. (2024, December). Italy's privacy watchdog fines OpenAI for ChatGPT's violations in collecting users' personal data. Apnews. https://apnews.com/article/italy-privacy-authority-openai-chatgpt-fine-6760575ae7a29a1dd22cc666f49e605f.

Zou, M., & Zhang, L. (2025, January). Navigating China's regulatory approach to generative artificial intelligence and large language models. In Cambridge Forum on AI: Law and Governance (Vol. 1, p. e8). Cambridge University Press.

Zulkifley, M. A., Munir, A. F., Abd Sukor, M. E., & Mohd Shafiai, M. H. (2023). A Survey on Stock Market Manipulation Detectors Using Artificial Intelligence. Computers, Materials & Continua, 75(2).