Legal Regulations on the Use of AI in Financial Services

Does the "Same Rule" Principle Necessitate New Laws and Regulations?

Wataru Tanaka

Abstract

This paper focuses on the need for laws and regulations on the use of AI in financial services. The discussion is primarily based on a review of previous research. The paper focuses in particular on whether, in the case of the application of the "same rule" principle, i.e., that "as long as similar services with similar risks are being provided, similar regulations should be imposed regardless of whether the services are provided by human beings or AI," the imposition of new laws and regulations for AI is actually necessary, and if so, what kind of laws and regulations need to be imposed and for what reasons. The main conclusion reached is that because the current legal framework, being based on the premise that only humans can act autonomously, is that only humans are subject to regulation, when an attempt is made to enforce the "same rule" principle, it might be necessary to institute new laws and regulations for AI so that negligence on the part of an AI results in the AI deployer bearing liability for damages.

Keywords: need for laws and regulations for AI, same rule principle, explainability, liability rules, liability of users

Contents

1. Introduction

With the rapid development of AI technology, the use of AI in various fields, including financial services, is on the rise (a definition of AI is provided in 2.1, but in this section, it is assumed to be computer system that learns and reasons with a certain degree of autonomy). AI has the potential to bring about major changes in society, but at the same time, there are concerns about its negative impacts, such as being used for crime and information manipulation or creating greater systemic risk. To ensure the sound development and use of AI technology, discussions on how to regulate it appropriately have been taking place around the world.

In Japan, AI regulation has hitherto centered on "soft law," e.g., government guidelines such as the AI Guidelines for Business (Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry (2024)) and industry self-regulations (AI Institutional Research Group of the AI Strategy Council (2025), p.3) However, major countries are also making progress with the development of laws and regulations (hard law), with a prime example being the Artificial Intelligence Act in the EU (below, "AI Act")[1] (for details of developments in the EU, see Buiten et al. (2023); Kretschmer (2023); Wachter (2024), and for details of developments in the U.S., see Brainard (2021); Hammer (2024)).

In Japan, the AI Institutional Research Group, operating under the Cabinet Office's AI Strategy Council, was established in July 2024, and is working on a regulatory framework for AI. Its mission encompasses "consideration of required laws and regulations based on risks" (Council for Science, Technology and Innovation of the Cabinet Office (2024), p.10). The Interim Report issued by the Research Group in February 2025 recommends that the government develop guidelines for AI in order to both promote innovation and address risks and conduct studies to comprehend the actual situation with AI. It also states that the implementation should be carried out through legal systems in order to ensure effectiveness (AI Institutional Research Group of the AI Strategy Council (2025), p.19). The Report also cites a survey from KPMG that found that only 13% of respondents in Japan "think that they can use AI safely under current rules and laws," the lowest percentage among major countries (AI Institutional Research Group of the AI Strategy Council (2025), p.4). Given such moves by the government and growing awareness among the general public, it appears possible that significant laws and regulations related to AI will be instituted in Japan in the future.

In light of the above, this paper seeks to explore the question of whether new laws and regulations for AI are necessary, and if so, what kind of laws and regulations are needed and for what reasons.

1 Artificial Intelligence Act (Regulation (EU) 2024/1689, https://artificialintelligenceact.eu/. The AI Act came into effect on August 1, 2024, with the provisions being phased in ahead of implementation of almost all them by August 2, 2026 (European Commission (2024)).

It constitutes a preliminary examination, being primarily based on a review of previous research. Below, in this section, I would like to state my basic view of the issues and my motivation for investigating them before I move on to the investigation itself.

In a report paper from the first Research Group on Technology and Financial Innovation (Tanaka (2022), hereinafter the "former paper"), I considered forms of regulation for online trading and robo-advisors, and introduced the principle of "same service, same risk, same rule" (below, the "same rule principle"), which asserts that "as long as the same services with the same risks are provided, the same regulations should apply, regardless of whether the service is provided by humans or machines," and expressed the view that regulations ought to be designed based on that principle (Tanaka (2022), pp. 58-59).

The same rule principle is not limited to online trading and robo-advisors, the subject of inquiry of the former paper, but is probably rational enough to serve as a design policy for laws and regulations for AI in general. This is because if the services provided by AI only pose the same level of risk as the same kind of services provided by humans, but are subject to stricter regulations than those provided by humans, AI-driven technological innovation will be hindered. And conversely, if laxer regulations are applied to services provided by AI than the same kind of services provided by humans, it will lead to excessive use of AI, such as using AI when it would have been cheaper for humans to provide those services. Both situations would undermine efficiency and cannot be considered desirable. As the Interim Report also makes clear, "regulations should not mandate or prioritize the use of specific types of technology in order to achieve their objectives." It states that regulatory approaches, including laws and regulations (hard law) should be considered with reference to the principle of "technical neutrality in regulations" (AI Institutional Research Group of the AI Strategy Council (2025), p.10).

As mentioned above, the same rule principle is likely to be rational, but the following questions arise: If the same rule principle is followed, and it is sufficient to consider the appropriate form of regulation according to the type of service provided and the degree of risk, will this not make it unnecessary to establish new "laws and regulations for AI" in the first place? If the rationality of the same rule principle is accepted, would there still be situations in which it is necessary to design new laws and regulations for AI? If so, what laws and regulations would be needed and for what reasons? In this paper, I would like to explore answers to the above questions by examining previous research that deals with the necessity and desirable form of laws and regulations for AI.

The paper is organized as follows: In section 2, after discussing what AI is, I briefly offer some examples of the use of AI in financial services. In section 3, I will present the conventional view on why laws and regulations are needed for AI, and then state my personal opinions on it. In section 4, after highlighting the existence of ex-ante regulation and ex-post regulation (liability rules) as basic categories of laws and regulations, I will describe what is being proposed as ex-ante regulation for financial services and the issues related to that. In section 5, I will discuss ex-post regulation (liability rules). Most importantly, I will express the view that if we want to enforce the same rule principle with regard to liability rules, which have hitherto been designed based on the premise that only humans can act autonomously,

they will need to be amended (through legal interpretation, and if necessary, legislation) to include AIs as autonomous actors. In section 6, I will set out the main results of my investigation, before bringing the paper to a close.

2. Significance of AI and its use in financial services

2.1 What is AI?

It is said that there is still no established definition of artificial intelligence (AI), but in general, it can be regarded as referring to computer programs or systems that work in a similar way to the thinking processes of humans (Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry (2024), p.9). However, especially in recent years, it seems that definitions have come to emphasize the characteristic of "autonomy." In other words, the term AI (or AI system) has started to be used to describe machines that rather than just making predictions and judgments according to rules set by humans (programs, algorithms), autonomously make inferences about patterns and laws through machine learning or deep learning based on large amounts of data, and based on these inferences, perform tasks such as making predictions, offering suggestions, and making decisions (Furukawa (2024), p.43).

The AI Guidelines for Business define an "AI system" as "a system (such as a machine, robot, and cloud system) that works at various levels of autonomy during the use process and incorporates a software element that has a learning function."

Meanwhile, "AI in the Guidelines is an abstract concept, which includes AI systems (as just defined) themselves or software or programs that perform machine learning" (Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry (2024), p.9). The definition of "AI system" in the EU AI Act also places emphasis on the function of autonomous inferencing (Furukawa (2024), p.43)[2].

2.2 AI categories

AI can be classified as specialized AI and general-purpose AI (AI Institutional Research Group of the AI Strategy Council (2025), p.5). Specialized AI is regarded as one that is specialized in performing specific tasks such as voice recognition, image recognition, or autonomous driving, while general-purpose AI is regarded as one trained on larger amount of data than specialized AI, has high versatility and can perform various tasks (AI Institutional Research Group of the AI Strategy Council (2025), p.5). Generative AI, whose potential has attracted a great deal of attention in recent years, is also regarded as belonging to general-purpose AI (AI Institutional Research Group of the AI Strategy Council (2025), p.5). Generative AI is described as "a general term representing AI developed from an AI model that can generate texts, images, programs, etc. (Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry (2024), p.9). See also Suga (2024), pp.8, 15).

2.3 Use of AI in financial services

The term AI is used in various ways in the financial services field (see Hammer (2024), pp.4-7; Okada et al. (2024), in addition to the examples of use presented below).

2 See EU AI Act, Article 3(1) ("'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. ").

For instance, as an example of use in credit screening, in October 2024, Seven Bank announced an initiative to conduct credit screening using the results of AI analysis by combining its own financial data with purchasing data provided by its parent company (Seven & i Holdings) (Nihon Keizai Shimbun (October 16, 2024).

In addition, with examples being the provision of investment advice and discretionary investment services by robo-advisors (Baker and Dellaert (2018); Tanaka (2022)), there are also increasing moves to employ AI for investment decisions and asset management (Bagattini et al. (2023); Dou et al. (2024)). According to a 2021 survey, 48% of hedge funds use AI to make investment decisions (Hammer (2024), p.5).

AI is also being used more and more for monitoring and risk management. For example, it has been reported that major credit card companies have developed fraud detection tools employing AI to prevent illicit transactions (*Business Insider Japan* (2024)), while banks are using AI to combat money laundering (Nikkei XTECH (2024)).

In recent years, generative AI has become a hot topic, and is already been used to check that advertisements for financial products are compliant with regulations, create internal documents such as approval requests, and respond to customer inquiries. (*Nihon Keizai Shimbun* (July 19, 2024)). And beyond financial services, generative AI is also seeing growing usage in audit services (*Nihon Keizai Shimbun* (June 4, 2024)).

3. Need for specific laws and regulations on the use of AI in financial services

3.1 What are the grounds for the need for specific laws and regulations for AI?

Next, I would like to consider this question: If new laws or regulations are imposed on the use of AI in financial services, what would the grounds for that be?

The same rule principle I introduced in section 1 is the idea that "as long as the same services with the same risks are provided, the same regulations should be imposed when they are provided by humans and when they are provided by AI." Conversely, according to this principle, if the provision of financial services by AI poses specific risks that are absent when humans provide the services, or if it poses risks that are typically greater than those posed when humans provide the services, it would be justified to impose stricter regulations on AI-provided services than on human-provided services.

But what specific risks might AI impose that would necessitate such specific laws and regulations? Traditionally, experts have emphasized the following two AI-specific risks:

(i) Opaqueness

The first is the issue of AI opaqueness (Hammer (2024), p.4). This is sometimes referred to as lack of model transparency or the black box problem (Brainard (2021), p.5). AI builds its own models (algorithms) based on data, and by doing so, is able to make various judgments in areas such as investment advice, credit screening, and insurance underwriting.

As a result, even the AI operator (provider or user of AI)[3] does not know how the AI made a specific judgment, so a situation may arise in which humans cannot properly control the behavior of AI (Hammer (2024), p.4; Brainard (2021), pp.5-6). This poses the danger that inappropriate behavior by AI (such as wrong predictions or judgments, or the generation of content that violates the rights of others) that is not prevented or corrected by humans may harm consumers and other people in society. In addition, it has been pointed out that there is a risk that victims will not be able to receive remedies because it would be unclear even after the fact that such harm was caused by inappropriate AI behavior (causality cannot be proven) (Buiten et al. (2023), p.6).

(ii) Data problems

Another AI risk that has been pointed out is problems related to data. AI extracts patterns from large amounts of data and performs operations such as prediction, decision-making, and content generation. It has been pointed out that this poses the risk of inappropriate behavior. For example, if the data used contains bias that disadvantages a specific group (specific race, gender, etc.), the AI model could amplify the bias, leading to discriminatory credit scoring and redlining (excluding a specific group from the service) (Brainard (2021), pp.4&7).

AI carries with it unique risks, i.e., opaqueness and data problems, and the argument that specific regulations , especially ex-ante regulations such as those described later in section 4, are needed because of these unique risks seems to be dominant in the discussion of AI regulation in Western countries today (Brainard (2021); Bagattini et al. (2023), pp.17-18; Hammer (2024)). However, there are questions about this. With respect to the problem of opaqueness, it can be said that humans are also a black box in terms of what kind of thinking processes they go through in their brains before making judgments. And humans can also make erroneous judgments when there is bias in the data on which those judgments are based. That being the case, the question must arise as to why the issues of black boxes and data bias are regarded as problems peculiar to AI.

3.2 Possibility that AI poses greater risks than humans

A possible answer to the question raised at the end of 3.1 is that while problems related to opaqueness and data are indeed common to both AI and humans, AI can perform a large number of operations based on a large amount of data in a small amount of time, so the harm caused to people in society of inappropriate behavior (e.g., the spreading of misinformation or discriminatory credit reviews) can be much greater than in the case of humans.

In addition, since the development and provision of AI systems require advanced technology and a large amount of data, it is expected that AI systems will be oligopolized by a small number of providers. Therefore, it is possible that all major securities market participants will use the same types of AI

3 In this paper, following the definitions used in the EU AI Act, I use the term "providers" to refer to developers of AI systems and those who provide AI services under their own names, and the term "deployers" to refer to those who use AI for business (Article 3(3) and (4) of the AI Act. Note that natural persons using AI for personal purposes are not included in "deployers."). Furthermore, I use the term "AI operators" to collectively refer to both. In the field of financial services, financial institutions that use AI are mainly deployers of AI, but some of their AI systems are developed in-house, so they may also be providers.

model for conducting transactions. It has been pointed out that this could lead to systemic risks such as triggering crowd behavior and chain reactions during market shocks and amplifying market volatility (Bagattini et al. (2023), p.17; Baker and Dellaert (2018), p.742)[4]. In addition, there is a view that multiple trading systems, through autonomous learning that allows them to predict each other's behavior, could engage in collusive price manipulation, triggering market price distortions and decreased liquidity (Dou et al. (2024)). Systemic risk and collusive price manipulation are, of course, not limited to AI, and can also be caused by humans, but it can be said that AI amplifies the danger.

In this way, the risks posed by AI are not necessarily qualitatively different from those posed by humans, but differences in the scale of risk can be said to exist. From that perspective, it may be possible to argue that imposing stricter regulations on AI than on humans (e.g., the ex-ante regulations mentioned in section 4) is rational to a certain degree.

3.3 Justification of specific laws and regulations for AI: an alternative perspective

Here, I would like to consider an explanation for justifying the imposition of specific laws and regulations for AI that differs from the one discussed in 3.2. Specifically, the fact that risks caused by opaqueness (black boxes) and data problems occur with both AI and humans, but in the case of AI, it is more likely that the risks can be reduced or eliminated with appropriate laws and regulations than in the case of humans (for an expression of a similar point of view, see Kleinberg et al. (2018)).

For example, given the existence of unconscious bias, it is not easy to eliminate discrimination caused by humans with laws and regulations. However, in the case of AI, laws and regulations may be able to completely eliminate discriminatory judgments during AI development or provision by imposing constraints on the data used for training or by making it mandatory to embed programs that prohibit judgments based on specific attributes (e.g., credit scoring based on race or gender). This reflects a key difference, namely that even before it becomes technically feasible, there are major legal and ethical constraints on manipulating human thinking (e.g., surgically operating on the brains of people with discriminatory tendencies to remove those tendencies), but there are no such constraints with AI, and it is also possible to make such manipulation mandatory as long as it is technically possible. In other words, rather than a difference in terms of the need for laws and regulations, it is the difference in the enforceability of laws and regulations (enforcement through laws and regulations is more often possible in the case of AI than in the case of humans) that justifies imposing laws and regulations on AI that are not imposed on humans. In the future, I would like to pursue research from such a perspective, but in this paper, I will limit myself to mentioning the ideas.

4 The Interim Report also expresses caution about the potential for AI to result in systemic risks: "As for systemic risks, large-scale AI systems in which multiple AI systems work together may support social systems in the future, and since if such groups of AI systems behave in unexpected ways, it could cause great confusion throughout the society, it is important to deal with such cases appropriately." (AI Institutional Research Group of the AI Strategy Council (2025), p.19).

4. Laws and regulations related to AI (1): ex-ante regulation

4.1 Introduction

Although there are questions such as those mentioned in 3.2, in general, it is likely that many think that it is rational to impose specific laws and regulations on AI because AI comes with the unique risks of opaqueness and data problems (See 3.1). In particular, one of the dominant views is that it is necessary to impose regulations (ex-ante regulation) requiring those who develop or provide AI or conduct business using AI to take certain steps to address AI risks in advance (Hammer (2024)), and some jurisdictions have already performed systematic ex-ante regulation, such as the EU with its AI Act.

In this section, 4, I will summarize the discussion on ex-ante regulation for AI. Note that among options for laws and regulations besides ex-ante regulation, regulations that impose liability for damages on AI operators when AI has actually caused harm (ex-post regulation or liability rules) are also important, but I will consider these in the next section, 5.

4.2 Risk-based approach

As a general method of ex-ante regulation, there is the risk-based approach, which classifies risks posed by AI according to their degree (intensity and scope), and imposes stricter ex-ante regulations on the use of AIs where the degree of risk is greater.

For example, Hammer (2024) divides risks posed by AI in financial services into three levels: high, medium, and low. As examples of high-risk AI, she cites propensity for bias or discrimination, significantly impact on financial markets, and possibility of large client losses. Medium-risk AI includes handling of sensitive customer information, privacy breaches, and potential for manipulation of customer behavior. Process automation and optimization fall into the category of low-risk AI. She also argues that the higher the risk an AI poses, the stricter the explainability (discussed later in 4.3) requirements should be for the financial institutions that use them (Hammer (2024), pp.11-12).

The EU AI Act (discussed above in note 1) is a representative example of a comprehensive ex-ante regulation based on a risk-based approach. The AI Act categorizes the risks of AI systems as "unacceptable risk," "high risk," "limited risk (or 'transparency risk')," and "minimal risk," with different levels of regulation imposed according to the degree of risk (European Commission (2024); Suzuki and Morita (2024); Furukawa (2024), p.41. See Fig. 1)[5].

The use of AI with "unacceptable risk" is prohibited (Article 5 of the AI Act). Examples of this are AIs

Fig. 1: EU AI Act risk classification

Degree of risk	Regulatory policy
"Unacceptable risk"	Prohibited
"High risk"	Regulated
"Limited risk" (transparency risk)	Transparency obligations
"Minimal risk"	Unregulated

Source: European Commission (2024)

5 In addition to the regulations to be described below in the main text of this paper, the AI Act stipulates special regulations for general-purpose AI (worded as "general-purpose AI models" in the Act) (Articles 51 to 56 of the same Act), but I will omit discussion of them here.

that use subliminal technology (paragraph 1 (a)of the same article) and certain AIs that perform social scoring, i.e., evaluate people's social behavior ((c)) of the same paragraph), see Furukawa (2024), pp.44-46.

Next, for "high-risk" AI systems, detailed ex-ante regulations are imposed, including the obligation to comply with "requirements" such as the establishment and operation of a risk management system, data governance, record keeping, and human monitoring (Articles 8 to 15, Article 16(a) of the same Act), as well as the obligation to register in the EU database before the start of services (Article 16(i) and Article 49 of the same Act)[6]. The AI systems classified as "high-risk" are specified in Article 6 and the Annexes of the AI Act (Habuka and Furukawa (2024), pp.96-98). Those related to financial services include "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud" (Article 6(2) and Annex III, paragraph 5(b) of the AI Act) and "AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance" ((c) of the same paragraph).

The AI Act also imposes transparency obligations, such as stipulating that when users interact directly with an AI system such as a chatbot (i.e., when there is "transparency risk"), they are informed that they are interacting with an AI (Article 50 of the AI Act. European Commission (2024)).

AI systems other than those subject to the above-described provisions are deemed to pose "minimal risk," and are not regulated under the AI Act (European Commission (2024)).

4.3 Explainability

In ex-ante regulation of AI, particular emphasis is placed on the requirement of "explainability" (Brainard (2021), pp.6-7; Hammer (2024), pp.9-12). This means being able to understand and interpret how AI models reach decisions and make predictions. The hope is that by requiring financial institutions to clearly explain their AI models, regulators will be better able to assess the potential risks of AI models and prevent AI from causing bias and erroneous judgments or posing systemic risks. Specific methods for explanation that have been proposed include future importance analysis, which identifies the input variables that have the most significant impact on the model's output; sensitivity analysis, which examines how changes in inputs affect the predictions; and rule extraction, which attempts to distill the model's decision-making process into a set of interpretable rules (Hammer (2024), p.10).

Hammer cites Basel regulations as well as relevant rules in the EU, U.S., and U.K. as examples of explainability requirements having already been incorporated into financial regulations in many jurisdictions (Hammer (2024), Appendix, pp. 15-21).

4.4 Problems with ex-ante regulation

However, problems and issues have also been pointed out with regard to ex-ante regulation. Since it is difficult for regulators to know in advance what actions it is appropriate for them to require operators to take to address AI system risks, there is a risk of too

6 Provisions concerning high-risk AI systems account for more than 85% of the total provisions of the AI Act (Habuka/Furukawa (2024), p.95). For details of regulations, see Habuka and Furukawa (2024), Furukawa and Habuka (2024), Arisaka (2024a) (2024b), and Yoshinaga (2024).

much or too little (from a cost-benefit perspective) ex-ante regulation, or of its content being unclear. And regarding AI-model explainability, which I discussed in 4.3, it has been pointed out that if the requirements are excessive, there is a risk that businesses will move away from more complex but potentially more effective AI models in favor of simpler, more easily explainable ones (Hammer (2024), p.12).

Kretschmer et al. criticize the ex-ante regulation in the EU AI Act (especially for high-risk AI systems), mainly on the grounds that it is complex and excessive. For example, Article 14 of the same Act requires "human oversight" as part of risk management for high-risk AI. Responding to this, Kretschmer et al. raise questions about whether the benefits of human oversight of AI systems can be expected to be commensurate with the burden of that oversight (such as psychological distress). They point to such issues as the fact that AI systems are often too vast for humans to evaluate every individual outcome and the fact that AI responses are so fast that it is often impossible to prevent errors through human oversight (Kretschmer et al. (2023), p.9)[7].

Reflecting on the criticisms they raise, Kretschmer et al. state that "it seems preferable to us to design sanctions arising from liability for harmful outcomes rather than impose ex-ante restrictions on specific actions," and recommend that AI risks be addressed by properly designing ex-post regulations (liability rules) rather than ex-ante regulations (Kretschmer et al. (2023), p.10). Next, I will examine the discussion of ex-post regulation (responsibility rules) for AI.

5. Laws and regulations related to AI (2): ex-post regulation

5.1 Significance of ex-post regulation (liability rules)

Ex-post regulation of AI, which I will explore in this section, refers to a legal framework that imposes liability for damages on AI operators (providers or deployers)[8] when AI has actually caused harm to customers or other people. In other words, it is the equivalent to the framework analyzed under the name "liability rules" in the fields of law and economics (Calabresi and Melamed (1972)). Well-designed liability rules have the function of improving efficiency or social welfare by, for example, providing incentives to those who engage in activities that are at risk of causing harm to people to take care to prevent such harm (Calabresi (1970); Shavell (2004) [Japanese translation 2010], chaps.8-12). Some leading researchers in law and economics argue that the state (government) often lacks sufficient information to conduct appropriate ex-ante regulation, and that it would be preferable to reduce ex-ante regulation and make greater use of liability rules (Shavell (2004), p.591 [Japanese translation 2010, p. 686]).

5.2 Issues with ex-post regulation for AI

However, issues have been pointed out concerning

7 Contrary to Kretschmer et al. (2023), discussed in the main text of this paper, there is criticism that the AI Act contains numerous loopholes, and fails to adequately address AI risks (Wachter (2024)).

8 See note 3 for the definitions of provider and deployer. The issue of how to apportion liability to the provider and the deployer for harm caused by AI is an important one in the design of liability rules, but is not dealt with in this paper due to constraints of space. See Kretschmer et al. (2023), pp.10-13.

the use of ex-post regulation (liability rules) for AI operators as a means of dealing with the risks posed by AI.

Specifically, except where strict liability (no-fault liability) is stipulated by specific laws (see, for example, Article 3 of the Product Liability Act[9]), current Japanese law adopts the principle of negligence/fault-based liability, meaning that liability for damages generally arises only in respect of harm caused by the willfulness or negligence (below, collectively, "negligence") of the perpetrator (see Article 709 of the Civil Code, which deals with general tort liability[10]. The same is true in major Western countries (Buiten et al. (2023), p.3)). Certainly, there is a liability rule for employers, which is that a person (employer) that employs another person (employee) for a business undertaking is liable to compensate for damage inflicted on a third party by their employee with respect to the execution of that business (Article 715, Paragraph 1 of the Civil Code). Although a proviso in the same paragraph stipulates that this does not apply if the employer can prove that they exercised reasonable care in appointing the employee or in supervising the business, or if the damage could not have been avoided even if the employer had exercised reasonable care, but in fact, it is said that such exemptions are rarely granted in court, and that being the case, it imposes no-fault liability on employers (Kubota (2018), p.205). However, the interpretation is that the premise for establishing employer liability is that the harm caused by the employee is assessed to be a tort (Kubota (2018), p.206). Therefore, it is generally understood that recognition that the harm caused to a third party was due to the employee's negligence (see Article 709) is needed to establish employer liability to be recognized that damage has occurred to the person.

In this way, it has been pointed out that under current law, which makes liability for harm caused by "human" negligence of the perpetrator (including the employee if the perpetrator is the employer) a requirement, then the more autonomy that AI acquires, i.e., the more AI can build algorithms from data and thereby make predictions, decisions, and even generate new content - the more difficult it becomes to deem that harm caused by AI is due to human negligence, which risks resulting in liability rules not functioning well (Buiten et al. (2023), p.7).

Seeking to address the above problems, in 2024 the EU amended the Product Liability Directive[11] to include intangibles such as software in the scope of "products" subject to regulation (Article 4(1) of the same Directive), enabling the rules of no-fault liability contained in the same Directive (For damage caused by defects in products, the manufacturer is liable regardless of whether there is negligence. Article 5 of the same directive.) to also be applied to AI (Buiten et al. (2023), pp.4-5). Furthermore, under the proposed AI Liability Directive[12] announced in 2022, if it is suspected that a high-risk AI system has caused damage, the AI operator (defendant) will have

9 The Product Liability Act, which was enacted in July 1998, stipulates that the manufacturer is generally (exceptions are stated in Article 4 of the same Act) liable for damage caused by a "defect" in their product, regardless of whether the defect was due to negligence (Article 3 of the same Act). This is a representative example of no-fault liability under a specific law. However, under the current Act, "products" are limited to "movables" (Article 2, paragraph 1 of the same Act), and is interpreted as not including intangibles such as software (Kubota (2018) p.269), so it would be difficult to hold an AI provider liable for harm caused by an AI error. For a discussion of how the recent amendment of the Product Liability Directive in the EU addresses this issue, see the part of the main text corresponding to note 11 below.

10 See Article 709 of the Civil Code ("A person that has intentionally or negligently infringed the rights or legally protected interests of another person is liable to compensate for damage resulting in consequence").

11 DIRECTIVE (EU) 2024/2853 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, (https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=OJ:L_202402853).

12 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)." COM (2022) 496 final 2022/0303 (COD) (September 28, 2022), (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0496).

to submit evidence to the court (Article 3 of the same proposed Directive), and it also includes a provision (Article 4(1) of the same Proposed Directive) to presume a causal link between the defendant's negligence and the damage if the defendant fails to submit evidence (Buiten et al. (2023), p. 5).

Such recent EU legislation (including that at the draft stage) will likely also serve as a reference for Japan as it considers the future design of ex-post regulation (liability rules). However, in this paper, I would like to describe and examine the proposal from Ayres and Balkin (2024), as it seems to be theoretically more interesting as a means of building liability rules that are aligned with the AI era.

5.3 Proposal from Ayres and Balkin (2024)

— AI as "agents without intentions"

Ayres and Balkin advocate the legal treatment of AI as "agents without intentions" as a solution to the problem of who is liable for harm caused by the use of AI and what the requirements for liability should be (Ayres and Balkin (2024), *1).

Under U.S. law, the focus of Ayres and Balkin's study, the standards for determining negligence and other forms of liability are generally objective. Therefore, even if there were no intention, as is the case with AI, it is possible to determine whether there was negligence by asking objectively whether reasonable care was taken (Ayres and Balkin (2024), *3). That being the case, if an AI is regarded as an agent, and the entity, such as a financial institution, that conducts business using the AI is regarded as the principal, agency law, under which the principal is liable for the agent's actions, can be applied[13]. Under agency law, when an agent performs duties under the control of a principal, the agent is considered an employee, and the principal is regarded as the employer[14], and if an employee commits a wrongful act within the scope of employment (which roughly corresponds to "with respect to the execution of that business" as stated in Article 715, paragraph 1 of the Japanese Civil Code), the employer bears vicarious liability, also known as respondeat superior, which is similar to the employer liability principle under Japanese law[15]. Therefore, if an AI were regarded as an agent (or even an employee) of the AI deployer, then the AI deployer would be deemed liable for harm caused by the AI to a third party through behavior objectively judged to be negligent (Ayres and Balkin (2024), p.*3).

Ayres and Balkin base their advocation of such liability rules on the contention that "people should not be able to obtain a reduced duty of care by substituting an AI agent for a human agent" (Ayres and Balkin (2024), p.*2). This is none other than the same rule principle.

13 For information on U.S. agency law, see Restatement (Third) of Agency (2006). See Higuchi and Sakuma (2014) for a Japanese translation and explanation of that Restatement. Also see Cox and Eisenberg (2019), Chap.1.

14 Restatement (Third) of Agency, section 7. 07(3).

15 Restatement (Third) of Agency, section 7. 07(1)(2); Cox and Eisenberg (2019), pp.30-33. Under U.S law (case law of each state), the scope within which an employer's vicarious liability is established does not necessarily coincide with the scope within which an employer's liability is established under Japanese law (some aspects of the former seem narrower than the latter), but I will omit a detailed comparison here. See Chap.9 [Norio Higuchi] in Higuchi and Sakuma (2014).

5.4 Rationality of proposal from Ayres and Balkin (2024)

I believe that Ayres and Balkin's proposal is rational enough to also be considered for adoption in Japanese law.

As mentioned in 5.1, under Japanese law, too, when an employee causes harm to a third party due to a tortious act in the execution of the employer's business, the employer is generally assumed to bear no-fault liability for compensation for damages (Article 715, paragraph 1 of the Civil Code. As already mentioned, the exemptions from liability provided for under the proviso in the same paragraph are rarely granted). Such employer liability has the function of improving efficiency by providing incentives for employers to take steps (care) to avoid harm through the selection and supervision of employees, and to reduce levels of business activities that are at risk of causing harm (Shavell (2004), p.233 [Japanese translation (2010), pp.266-267]). In particular, making employer liability no-fault liability rather than negligence is rational because employers often have more information than the state (courts) about what steps they should have employees take to avoid harm (Shavell (2004), p.234 [Japanese translation (2010), pp.268–269]), and because doing so would not only encourage appropriate levels of care but also ensure that businesses adjust their overall activity efficiently (see Shavell (2004), Chap.8, sec.4 [Japanese translation (2010), pp.221–228])[16]. And in accordance with the same rule principle, such employer liability should be applied regardless of whether the person/thing used by the business operator is a human or an AI.

Furthermore, in Japanese law, negligence is generally understood not as a subjective state, such as a lack of mental alertness, but rather as an objective behavior, such as a failure to take the necessary steps to prevent harm (i.e., a violation of the obligation to avoid harmful outcomes) (Hirai (1994), p.28, Kubota (2018), p.46). According to such understanding of negligence, it is possible to conceptualize "negligence of AI" by realizing that if an AI's actions (prediction, decision-making, content creation, etc.) would have been deemed negligent if a human had performed them under the same circumstances, those actions of the AI would also be negligent.

For example, services where customers ask and receive answers to questions via a generative-AI chatbot have already been deployed by many financial institutions (Okada et al. (2024)), but if the AI responds falsely and causes harm to a customer as a result, it should be viewed as a tort just as it would be if it were a human that had responded falsely, and the financial institution deploying the AI should bear liability for damages to the customer. Furthermore, it is likely that in the future it will become normal for AI to explain financial products to customers and even solicit purchases of them, but should that happen, if the AI's explanations contravene the obligation to explain (see Article 37, paragraph 3 of the Financial Instruments and Exchange Act [FIEA] / Article 117, paragraph 1, item (i) of the Cabinet Office Order on Financial Instruments Business, Article 4, paragraph 1 of the Act on the Provision of Financial Services, see Iida (2023), pp.398-399), or its solicitations seriously violate the principle of suitability (Article 40, paragraph 1 of the FIEA)[17],

16 See Sykes (1984) for a detailed analysis of the significance (function) of employer liability (vicarious liability in Anglo-American law) as described in the main text of this paper.

17 Although Article 40, paragraph 1 of the FIEA, which stipulates the principle of suitability, is itself an administrative regulation related to businesses, a court ruling has deemed that when a financial instruments business operator, etc. solicits a financial instruments transaction that significantly deviates from the principle of suitability, it is illegal under tort law, too, and liability for damages will arise (Supreme Court of Japan ruling dated July 14, 2005, published in Vol. 59, Issue 6, p.1,323 of the *Minshu* (Reports of the Supreme Court)). See Iida (2023), pp.407-410.

then as would be the case if a human employee had given such an explanation or made such a solicitation, the financial institution deploying the AI should bear liability for damages to the customer.

5.5 Reform of laws and regulations to enforce the "same rule" principle

The question is whether the liability rule that "AI deployers are liable for damages based on the negligence of the AI (including the violation of various legal requirements such as the obligation to explain, the principle of suitability, etc.)" is enforceable as an interpretation of current Japanese law.

In this regard, it seems that "employee" as referred to in Article 715, paragraph 1 of the Civil Code has naturally been assumed to be a human being. However, the same paragraph does not contain a specific definition of "employee," and the concept of employee has been long been interpreted flexibly, such as it being deemed that the employer/employee relationship described in Article 715 of the Civil Code can be established without an employment contract (Kubota (2018), p.208). Given this, it seems that today, when AI is gaining more and more autonomy due to advances in technology, the paragraph could be applied to both AIs and (human) employees.

Another option that seems to be enforceable as an interpretation of the current law is to directly assume that when an AI has behaved in a way that can be considered negligence (including the violation of various legal requirements), it is negligence on the part of the AI deployer itself (usually a juridical person), and to recognize tort liability under Article 709 of the Civil Code as being borne by the AI deployer itself. Regarding the question of whether it is possible to admit "tortious acts of a juridical person itself," there have been conflicting court rulings and theoretical disputes (Hirai (1994), pp.226-227). Nevertheless, an prevailing scholarly view holds that, as a matter of legal interpretation, such tortious acts of a judicial person should be admitted to some degree in order to facilitate victim compensation in situations where the negligence of individual employees of the corporation cannot be established, thereby impeding the pursuit of liability under Article 715, Paragraph 1 of the Civil Code (Hashimoto (2016). Today, when the concept of negligence is objectified, if it is recognized that juridical person did not take the measures it should have taken to avoid harm (i.e., there was a violation of the obligation to avoid harmful outcomes), it would appear possible to recognize that the juridical person itself was negligent, without any need to attribute blame to any specific person. In the future, as the use of autonomous AI expands, it would seem possible that such legal interpretations could be increasingly accepted.

However, the interpretation that "employee" in Article 715, paragraph 1 of the Civil Code includes non-human beings has so far not been asserted by anyone, and it is unclear whether such an interpretation could be adopted in judicial decision-making, and even if it could, when this could happen. In addition, there's also a strong view that denies tortious acts of a judicial person itself, arguing that to determine whether there's a breach of duty of care—which is a prerequisite for negligence—the actions of a natural person must be at issue. (Hirai (1994), p.227).

If it would be difficult to establish a rule that "liability for damages of an AI deployer arises based on the negligence of the AI" as an interpretation of current law, then in order to enforce the same rule principle, legislation to explicitly recognize such a rule would be necessary. This may be one of the cases where the same rule principle would require new laws and regulations for AI. In other words, as long as the same services with the same risks are being provided, the same regulations should be imposed regardless of whether the services are provided by human beings or AI, but under current law, the premise that only

humans can act autonomously (which had hitherto not been doubted), the rule only applies to cases where a human is the actor. Therefore, to enforce the same rule principle, there will be cases where new laws and regulations, particularly for AI, become necessary.

6. Conclusion

This paper has provided an overview of the debate surrounding laws and regulations for the use of AI in financial services from the point of view of the question of whether if the same rule principle is applied, i.e., "as long as the same services with the same risks are being provided, the same regulations should be imposed regardless of whether the services are provided by human beings or AI," is the imposition of new laws and regulations for AI actually necessary? In response to the above question, this paper has yielded some answers, which can be summarized as follows:

(i) Regarding AI, the view that specific laws and regulations are necessary on the grounds of unique risks posed by opaqueness and data problems is influential, but these risks also exist for humans. However, due to the nature of AI, which is capable of processing large amounts of data instantaneously, these risks may be amplified compared to humans. This might justify the imposition of specific laws and regulations for AI (3.2).

(ii) As an alternative point of view to (i), in the case of AI, it may be easier to employ legal regulation to eliminate or mitigate the above-mentioned risks than it would be in the case of humans. In this way, in light of the difference in enforceability, rather than the necessity of laws and regulations, it may be possible to justify imposing laws and regulations on AI that are not imposed on humans. (3. 3).

(iii) The current legal framework, being based on the premise that only humans can act autonomously, features rules, applied in certain cases, that only humans are subject to regulation. Therefore, if the intent is to enforce the same rule principle, there could be cases where new laws and regulations that cover not only humans but also AI become necessary. Specifically, to enforce a rule that "liability for damages of an AI deployer arises based on the negligence of the AI," new legislation might be required (5.5).

The discussion in this paper has constituted no more than a preliminary examination based on a review of the limited literature available. In the future, I intend to conduct further research on the use of AI in financial services, and dive deeper into exploring the issue of what kind of regulation would be appropriate.

References

Japanese language:

AI Institutional Research Group of the AI Strategy Council (2025), "Interim Report" (February 4, 2025), (https://www8.cao.go.jp/cstp/ai/interim_report.pdf)

Business Insider Japan (2024), "Utilizing Generative AI in the Workplace: Nine Companies Whose Profitability Has Already Begun to Improve. - Bank of America Analysis," *Business Insider Japan Premium*, August 21, 2024 [available via Nikkei Telecom 21]

Yoko Arisaka (2024a), "Overview of EU AI Act (4th): Obligations of Providers (Articles 16-22)," *NBL*, No.1273, pp.89-97

Yoko Arisaka (2024b), "Overview of EU AI Act (5th): Obligations of Importers and Sellers (Articles 23-39)," *NBL*, No.1274, pp.76-83

Hidefusa Iida (2023), *Financial Instruments and Exchange Act*, Shinsei-sha

Takuro Okada, Ichio Sato, and Toshiyuki Yamamoto (2024), "Panel Discussion on Use of AI in the Financial Sector and at Financial Institutions,"

Financial Legal Affairs, No.2231, pp.23-34
Atsumi Kubota (2018), "Tort Law (2nd Edition)," Yuhikaku
Chizuru Suga (2024), "Transformation of Japanese Society by Generative AI: Keynote Lecture," *Financial Legal Affairs*, No.2231 pp.8-22
Shohei Suzuki and Hiroyuka Morita (2024), "Overview of the European AI Act," (May 27, 2024), (TMI Associates blog) (https://www.tmi.gr.jp/eyes/blog/2024/15787. html
Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry (2024), "AI Guidelines for Business (Version 1.01)" (November 22, 2024) (https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20241122_1.pdf).
Wataru Tanaka (2022), "The Social Significance of Regulatory Approach to Technological Innovation in the Retail Field: Focus on Internet Trading and Robo-Advisors," *JSRI Journal of Financial and Securities Markets*, No.119, pp.45-64
Hiroki Habuka and Naohiro Furukawa (2024), "Overview of EU AI Act (2nd): High-Risk AI Classification and Requirements for High-Risk AI (Articles 6-10)," *NBL*, No.1270, pp.95-102
Norio Higuchi and Takeshi Sakuma (2014), *Modern Agency Law: U.S. and Japan*, Kobundo
Yoshio Hirai (1992), *Theories of Claims II: Torts*, Kobundo
Naohiro Furukawa (2024), "Overview of EU AI Act (1st): General Provisions and Prohibited AI (Articles 1-5)," *NBL*, No.1269, pp.40-46
Naohiro Furukawa and Hiroki Habuka (2024), "Overview of EU AI Act (3rd): High-Risk AI Classification and Requirements for High-Risk AI (Articles 11-15)," *NBL*, No.1271, pp.101-108
Council for Science, Technology and Innovation of the Cabinet Office (2024), "Current Situation and Institutional Issues of AI Policy," Handout Material 1 at the Joint Meeting of the AI Strategy Council (11th) and the AI Institutional Research Group (1st) (held on August 2, 2024), (https://www8.cao.go.jp/cstp/ai/ai_senryaku/11kai/shiryo1.pdf)
Nikkei XTECH (2024), "Resona Holdings Using AI to Tackle Money Laundering Ahead of Next FATFS Evaluation," June 27, 2024 [available via Nikkei Telecom 21]
Nihon Keizai Shimbun (June 4, 2024), "Audit Firm Enhances Business Efficiency with Generative AI: KPMG AZSA Achieves 220,000 Reduction in Man-Hours," *Nihon Keizai Shimbun Electronic Edition*, June 4, 2024
Nihon Keizai Shimbun (July 19, 2024), "Nomura Using Generative AI to Review Advertisements, Mizuho Saving 2,000 Man-Hours per Month," *Nihon Keizai Shimbun Electronic Edition*, July 19, 2024
Nihon Keizai Shimbun (October 16, 2024), "Seven Bank Trials Use of '7iD' Purchasing Data for Card Loan Credit Screening," *Nihon Keizai Shimbun Electronic Edition*, October 16, 2024
Yoshiyuki Hashimoto (2016), "Reconsideration of 'Tortious Acts by Juridical Persons Themselves:" Overall Liability Rules for Business Organizations," *Quarterly Jurist*, No.16, pp.50-60
Kyoko Yoshinaga (2024), "Overview of EU AI Act (6th): High-Risk AI Standards, Conformity Assessment, Certificates, Registration (Articles 40-49), Transparency Obligations for Providers and Deployers of Certain AI Systems (Article 50)," *NBL*, No.1275), pp.67-78.

English language:

Ayres, I. and Balkin, J. M.（2024）, "The Law of AI is the Law of Risky Agents Without Intentions," University of Chicago Law Review Online, *1-*11 （ 11/27/2024 ）, https://lawreview.uchicago. edu/sites/default/files/2024-11/Ayres_Balkin_ Law%20of%20Risky%20Agents.pdf.
Bagattini, G., Benetti, Z., and Guagliano, C.（2023）, "Artificial Intelligence in EU Securities Mar- kets," ESMA Report on Trends, Risks and Vulnerabilities Risk Analysis （1 February 2023 ）, available at https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf.
Baker, T., and Dellaert, B.（2018）, "Regulating Robo Advice across the Financial Services Industry," Iowa Law Review 103 (2) : 713-750.
Brainard, L.（2021）, "Supporting Responsible Use of AI and Equitable Outcomes in Financial Services," at the AI Academic Symposium hosted by the Board of Governors of the Federal Re- serve System, Washington, D.C., Virtual Event （January 12, 2021 ）, available at https://www.federalreserve.gov/newsevents/speech/brainard 20210112a.htm.

Buiten, de Streel, Alexandre, d.S., and Peitz, M.（2023）, "The Law and Economics of AI Liability," Computer Law & Security Review 48 : 105794.

Calabresi, G.（1970）, The Costs of Accidents : A Legal and Economic Analysis, Yale University Press.

Calabresi, G., and D. Melamed, D.（1972）, "Property Rules, Liability Rules and Inalienability : One View of the Cathedral," Harvard Law Review 85 : 1089-1128.

Cox, J.D., and Eisenberg, M.A.（2019）, Business Organizations : Cases and Materials（12 th ed.）, Foundation Press.

Dou, W. W., Itay, G., and Ji, Y.（2024）, "AI-Powered Trading, Algorithmic Collusion, and Price Efficiency," Jacobs Levy Equity Management Center for Quantitative Financial Research Paper , The Wharton School Research Paper （May 30, 2024）, Available at SSRN : https://ssrn.com/abstract=4452704 or http://dx.doi.org/10.2139/ssrn.4452704.

European Commission（2024）, "AI Act," https:// digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

Hammer, S.（2024）, "Navigating the Neural Network: Artificial Intelligence in Finance and Recalibration of the Regulatory Framework," Penn Program on Regulation Research Paper Series No.24-01 （ October 2024 ） , https://pennreg.org/wp-content/uploads/2024/10/Hammer-Navigating-the-Neural-Network.pdf ［ forthcoming : in P Hacker,P., Engel, A., Hammer, S., and Mittel- stadt, B.（eds）, The Oxford Handbook on the Foundations and Regulation of Generative AI（Oxford University Press）］

Kleinberg, J., Ludwig, J., Mullainathan, S., and Sun- stein, C.R.（2018）, "Discrimination in the Age of Algorithms," Journal of Legal Analysis 10 ⑵ : 1-62.

Kretschmer, M., Kretschmer, T., Peukert, A., and Peukert, C.（2023）, "The Risks of Risk-based AI Regulation: Taking Liability Seriously（" September 27, 2023）. Available at SSRN : https://ssrn. com/abstract=4622405 or http://dx.doi.org/10.2139/ssrn.4622405

Shavell, S.（2004）, Foundations of Economic Analysis of Law, Belknap Press of Harvard University Press ［ Japanese translation also available, translated by the author and Takashi Iida and published by Nikkei Business Publications in 2010］

Sykes, A. O.（1984）, "The Economics of Vicarious Liability," Yale Law Journal 93 ⑺ : 1231-1282.

Wachter, S.（2024）, "Limitations and Loopholes in the EU AI Act and AI Liability Directives : What This Means for the European Union, the United States, and Beyond," Yale Journal of Law & Technology 26 ⑶ : 671-718.

(Professor, Institute of Social Science, University of Tokyo)