Advantage of Japanese approach to AI regulation

Ryoji Kashiwagi

10 September 2024

Iakyara vol.390

Nomura Research Institute, Ltd.

Executive Summary

Recent rapid advances in generative AI are eliciting growing concerns about risks posed by it. In response, governments are working on adopting regulations to mitigate such risks. Japan's generative AI regulatory framework lowers barriers to entry to the AI market while placing priority on the quality of generative AI output, thereby facilitating generative AI's sound development without impeding innovation.

Ryoji Kashiwagi
Expert Researcher
Financial Market & Digital Business Research Department

Generative AI regulation from standpoint of AI model lifecycle

In the wake of ongoing rapid advances in generative AI, governments worldwide are drafting regulations to promote its sound development in response to growing concerns about the risks it poses[1]. Below we discuss regulation of generative AI through the lens of generative AI models' lifecycle.

The generative AI lifecycle can be broadly divided into three phases: model development/training, model optimization and production. In the development/training phase, a trained model is built by amassing huge datasets and deploying large-scale computing resources to train the model based on the data, which is usually text or images. In the optimization phase, the trained model is variously adjusted to enable it to provide more accurate and idiomatic answers. In the production phase, the tuned model generates output (e.g., text, images) in response to real-life users' questions or prompts.

Regulatory focal points differ across these three phases. In the development/training phase, the key issues revolve around the data used to train generative AI models, most notably issues pertaining to use of copyrighted content and handling of personal and other sensitive information. Another issue is exclusion of erroneous, biased or otherwise low-quality data from training datasets. In the optimization phase, regulatory priorities include ensuring that generative AI models are free from ethically problematic biases and do not generate erroneous output out of carelessness or behave in other ways unintended by their developers. The optimization phase has considerable overlap with the production phase in terms of regulatory focus. In the production phase, regulators are concerned about the risk of ethically problematic or erroneous output (in addition to deep fakes) and

NOTE
1) At the G7 Hiroshima Summit in May 2023, the G7 drafted a set of universal rules for generative AI utilization/regulation broadly applicable to generative AI developers and commercial users. The Hiroshima AI Process calls for AI developers and commercial users to assess AI risks, adopt risk-based approaches, publicly disclose information, implement security measures, protect personal information and honor copyrights.

copyright infringement by generative AI output (or copyrighting of generative AI output[2]).

2) Many countries have a policy against copyrighting of generative AI output. In China, however, some generative AI output can be copyrighted under common law.

It's important to note that regulations concerning generative AI are not uniformly applied to all models. The stringency or leniency of these regulations can vary depending on the specific risks associated with the use case. Generative AI regulatory frameworks often adopt a risk-based approach to address these differences.

Generative AI regulations in EU and US

<EU>

The EU's new AI Act, passed by the European Parliament in June 2023, is slated to fully take effect in 2026. It places priority on safeguarding human rights and freedoms in the EU based on the fundamental principle that technology should be human-centric. It takes a risk-based approach and, like other EU regulations (e.g., the GDPR), applies even to AI models offered by companies domiciled outside the EU.

The AI Act will likely require AI training data to comply with the GDPR and impose significant restrictions on access to a wide variety of training data. Additionally, high-risk AI models must be registered with the EU and providers of such systems will be required to have a quality control process in place that encompasses the system's production phase also.

Under the AI Act, generative AI will be subject to quite stringent regulation. Non-EU companies in particular face formidable regulatory challenges. In fact, Apple announced in June that it will initially hold off on offering certain AI features in the EU out of concern about privacy protection regulations. Less than a month later, Meta announced it will not roll out multimodal AI models in the EU. These announcements have raised concerns about the EU missing out on some AI technologies.

<US>

In the US, President Biden issued an executive order on AI in October 2023. This Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence calls for standards to be established for testing generative AI

models in their development/training phase and requires AI developers to disclose the test results and other key information to the federal government. It also requires companies developing AI models that pose material national-security or other risks to report to the government on the model's development process.

The Executive Order is strictly an administrative directive, not new regulatory legislation. As such, it provides a regulatory framework that arguably places more emphasis on promoting innovation than the EU's AI Act does. Republicans, however, want to revoke Biden's AI executive order. Trump allies are reportedly drafting a new executive order that has been framed as the AI equivalent of the Manhattan Project. How AI regulation ultimately shakes out in the US remains to be seen.

Opportunities presented by Japanese regulatory approach

Japan does not yet have a comprehensive regulatory framework for generative AI, but Japanese policymakers have started discussing generative AI regulation in response to overseas regulatory developments. The framework under discussion is largely modeled after the Hiroshima AI Process. Points on which consensus has yet to be reached include whether to adopt a risk-based approach, information exchanges between companies and the government, and monetary penalties.

The most distinctive feature of Japan's current regulations governing generative AI is how textual works are treated in the AI development/training phase. Japan's Copyright Act contains a fair-use exception for information analysis. As a general rule, mass use of copyrighted textual content is permitted in Japan if its purpose is information analysis. This provision enables AI developers to comprehensively analyze, e.g., social media content, academic papers or news articles within the Copyright Act's purview. This fair-use exception for information analysis may lower barriers to entry to the AI market and facilitate more effective training of AI models.

Access to high-quality training data is a crucial determinant of competitiveness in the generative AI space. Recently, however, data owners have been increasingly opposed to their data being freely used by AI developers[3]. In Japan, by contrast, AI developers have the advantage of being able to access training data without worrying about copyright infringement. We hope Japan pursues policies that capitalize on that advantage. At the same time, Japan must of course build a regulatory regime that deals harshly with copyright infringement by production-phase AI models.

3) *Data needed to develop AI is rapidly drying up, with a quarter of high-quality data becoming unusable in just one year,* Gigazine (July 23, 2024). https://gigazine.net/gsc_news/en/20240723-ai-data-restrictions/

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.9 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 17,400 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Digital Business Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/fis/lakyara/