Publishing of a working draft of a "Basic Law for Promoting Responsible AI" submitted to a project team of the Liberal Democratic Party of Japan

Atsumi & Sakai
Policy Research Institute

In January 2023, the Liberal Democratic Party of Japan launched a project team ("AIPT") on the evolution and implementation of AI, led by Masaki Taira, a member of the House of Representatives, to consider Japan's AI strategy and policy recommendations. Based on these considerations, AIPT member's a private proposal for new legal governance in our country, specifically targeting particularly powerful generative AIs (called "frontier AI models"). has been submitted to AIPT and published as the "Basic Law for Promoting Responsible AI"[1]. The Draft AI bill will regulate developers of foundation AI models of a certain scale and purpose.

The Draft AI bill aims to balance risks and benefits brought about by AI through the introduction of appropriate AI governance. Specifically, it seeks to restrict risks of infringement on the rights and interests of citizens, while maximizing the benefits of healthy AI development, including AI-driven innovation. This is to be achieved by public-private joint regulation against developers of specific foundation AI on sharing of risk information, establishment of a governance-system, disclosure, and so on.

The bill specifically targets so-called "specific AI foundational models" with significant social impact, known as frontier AI models. It does not intend to include small-scale models or startups. The discussion points include the necessity and acceptability of regulating the developers of foundational models, how to evaluate and classify based on "scale" and "purpose" (e.g., number of parameters, training data, whether the model is for general purposes, etc.). In addition, whether Japanese government regulates by designating unilaterally or requiring prior notification, sanctions for non-compliant developers, and the geographical scope of application are important continuous discussion points.

Companies developing specific AI foundational models are required to establish seven measures, including third-party vulnerability verification and disclosure of the model's basic specifications, which align with commitments made voluntarily to the U.S. government by major AI companies last year.

---

[1] https://note.com/masanao_ozaki/n/nbd4dd013a5cb
https://note.com/api/v2/attachments/download/85055711b2ebdae1585d4e7345ac5a70

These seven measures are:

1. **Conduct safety verification (e.g., red team testing) by the company and externally for AI in particularly high-risk areas.**

2. **Share risk information between companies and the government.**

3. **Invest in cybersecurity to protect unpublished weights.**

4. **Detection and reporting of vulnerabilities by third parties.**

5. **Implementing mechanisms to notify users of the use of generative AI.**

6. **Disclosure of AI's capabilities and limitations.**

7. **Promotion of research on the social risks of AI.**

However, specific standards for these measures (e.g., scale and frequency of red team tests, level of cybersecurity, etc.) are expected to be determined by the private sector, including business associations, to keep up with the speed of technological advancement. This regulatory system, where the government defines what to do and the private sector determines how to do it, is generally known as a "co-regulation" model.

Developers of specific AI foundational models are required to regularly report to the government (or the newly established AI Safety Institute by IPA[2]) on their compliance with these measures. The government will review these reports and, if necessary, make them public or provide guidance and supervision. Violations of reporting obligations or orders may result in fines or criminal penalties. Unlike European AI regulations, this bill does not envisage immediately banning or imposing regulations on specific AI foundational models or services based on their content.

---

[2] https://aisi.go.jp/

In relation to topics on AI regulations and guidelines, Japan's Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI) have published draft unified government guidelines based on discussions at the Hiroshima AI process in January 2024[3]. These guidelines, which call for voluntary efforts, are not limited in applicability, in contrast to the AI bill. The guidelines maintain the current concepts of the OECD AI principles and the Japanese Principle of Human-Centric AI. The guidelines are unique in that they add new requirements to the advanced AI model (the requirements are basically in line with the Hiroshima AI process), adjust the description of the MIC's AI development and utilization principles in light of the progress of generative AI, and require agile governance with regard to the use of such conventional principles. Agile governance is the concept that calls for continuous improvement based on assessment of technical and social changes.

In line with concept of agile governance, the Japanese government and Japanese politicians are trying to develop appropriate national regulations and internal systems at companies in response to changes in technological and social risks, and changes in international trends through the consideration of new legislation and guidelines, without establishing overly strict ex ante regulations.

----

[3] https://www.soumu.go.jp/main_content/000923717.pdf
https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

Authors/Contacts

Takafumi Ochiai

Atsumi & Sakai

Head of Policy Research Institute

E: **takafumi.ochiai@aplaw.jp**

Tatsuhiro Hirayama

Atsumi & Sakai

Policy Research Institute

Principal Researcher

E: **tatsuhiro.hirayama@aplaw.jp**

If you would like to sign up for Policy Research Institute Newsletters, please fill out the sign-up form.

Back issues of our newsletters are available here.