

Some comments on AI governance

Tomoyo Matsui
U.Tokyo Japan

What is digital governance?

“Our focus is on corporate governance issues vis-à-vis AI and data security because although companies are dealing with a host of tech related issues that are relevant for corporate governance, these are the two most significant areas. Further, corporate governance today has to consider technology across two verticals – first, the use of technology within corporate governance, and second, factoring in the risks of using technology in corporate activity. We consider both these verticals in this paper. For short, we will refer to these governance challenges faced by companies and any measures taken to deal with them, as ‘digital governance’”.

Merits and risks associated with the use of technology within corporate governance. .

Problems occurring around with the decision to use digital technology in corporate activity.

Brief overview of the problems

① Data Security (whether the AI solve the problems successfully or not is not the question here)

We need data to feed AI. The basic risks are : domestic problem (data breach (data theft & information leak) and ambiguous algorithm architecture) and international data transfer issue.

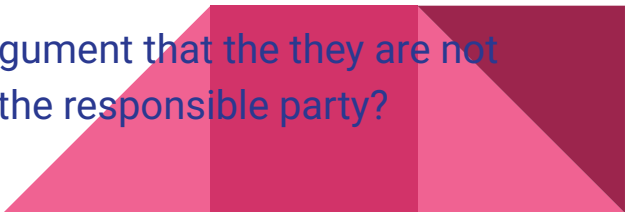
② Civil (or corporate) liability for poorly introduced AI and damage compensation

We have to have a clear view what the actual damage-inducing factor was. Biased algorithm? Incomplete dataset? Poorly made decision to introduce AI to an inappropriate situation? (AI or data providers are different entities from the corporation itself.)

③ Insufficient human resources supporting AI application, at both the engineering and the management level.

If in-house engineers are not capable of checking the AI, how can companies avoid the risk of accepting ill-performing AIs?

If monitoring organs are not capable and managers stick to the argument that they are not liable when AI fails, who can see through the situation and pin down the responsible party?



Data Security : domestic and transnational

①Data Security (whether we should use AI to solve problems or not is not the question here)

We need data to feed AI. The basic risks are : domestic problem (data breach (data theft & information leak) and ambiguous algorithm architecture) and international data transfer issue.

1.“AI training data must come from lawful sources and must not infringe on intellectual property rights or user privacy.”(footnote 42)

China/ industry-by-industry basis regulation encompasses from data protection to algorithmic transparency obligation.

India/ industry-based regulation, data-protection best practices under working.

2. “enterprises must conduct security assessments and mitigate risks before providing data to overseas entities, ensuring the lawful and orderly flow of data.”(footnote 44)

China/ regulate the outbound data transfer, demand risk assessment

India/ liberal approach regarding data localisation.(transfer possible to all countries except those that were restricted by the government. However, in January 2025, MeitY notified draft rules under the DPDPA which allow for more ad hoc restrictions.)

Liability and governance structure

② Liability for inadequately introduced AI and damage compensation thereof

We have to have a clear view what the actual damage-inducing factor was. Biased algorithm? Incomplete dataset? Poorly made decision to introduce AI to an inappropriate situation? (AI or data providers are different entities from the corporation itself.)

Similar situation in China and India.

③ Insufficient human resources supporting AI application, at both the engineering and the management level.

If in-house engineers are not capable of checking the AI, how can companies avoid the risk of accepting ill-performing AIs?

If managers can argue that they are not liable when AI fails, who can see through the situation and pin down the responsible party?

China/ audit or risk (management) committee, internal control and disclosure

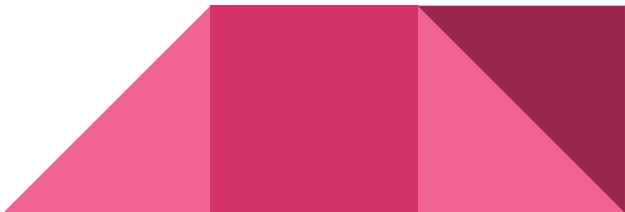
India/ CTOs (Chief Technology Officers) numerical data on recent breach-report cases

Situation in Japan

① Regulation on AI itself

Revised Personal Information Protection Law (periodical assessment by every 3 years)・・・ The main purpose of the regulation is to encourage defense against cyber attacks and define what to do if you are a victim of a cyber attack. (2024 major regulatory progress: AI business guideline / Caution for cloud service providers etc.)

Smooth International Data transfer vs. localization Countries that prevent their own data from being leaked outside their borders and coalitions of countries that allow data to flow through mutual authentication are forming different localized data distribution spheres. Japan is making alliances with EU, UK and some other countries.



Situation in Japan

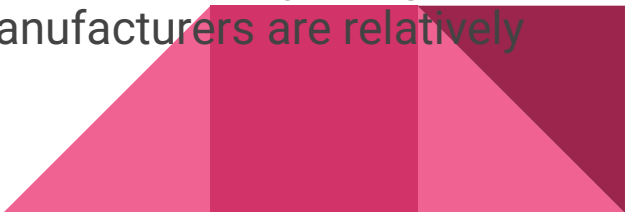
② Distribution of responsibility among separate players (piecemeal approach)

Digital Platform Providers are required to provide explanation on their algorithm structure (Anti-competition guideline and case law on the matter of abuse of dominant bargaining position)

Autonomous vehicle transportation is showing gradual progress (Professor Fujita(editor)'s detailed report/book on civil liability distribution)

③ Scarce supply of AI-savvy staffs both at operational and executive level

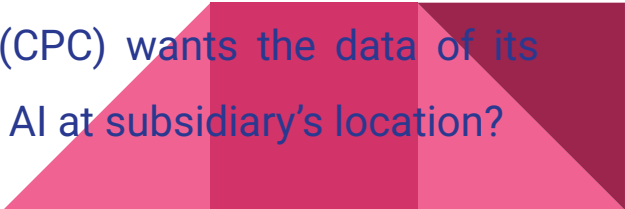
Japanese company is slowly attempting to introduce AIs to low-risk operations such as customer information center or secretarial operations such as adjusting schedule or taking minutes of various meetings. Product manufacturers are relatively active in introducing AIs in manufacturing operations.



Some questions

Many EU, UK or US countries have long maintained Indian transacting parties that operate as their outsourced customer service operations or as call centres, which helped AI industry to flourish in India. But China has tech giants that can lay out domestic data centre. It seems that China and India is adopting different approach to international data transfer and are thus belonging to different data-flow sphere.

Pure hypothetical case: An Indian parent company (IPC) wants a streamlined operation throughout the group companies with the use of an AI and needs the data of its subsidiary located in China. Will IPC decide that AI be used in India (at parent company) or in China (at subsidiary)? On the other hand, if a Chinese parent company (CPC) wants the data of its subsidiary located in India, will CPC choose to feed data to Indian AI at subsidiary's location?




Some questions (cont'd)

About data protection(cont'd) : If the manner of handling data is uneven across countries and undermines equal footings in trade, won't this give rise to any problems in terms of free trade, described in many agreements such as those under the WTO and EPA ? What do you think the AI-related transnational data flow will be like in the future?

About civil liability: Are there some academic discussions, even piecemeal-approach ones, on how an AI-related civil liability should be distributed among incapable AI-developer, poorly-equipped data-provider, business corporation that falsely applied AI to product development, customers that misused the AI-programmed product, and insurers? For example, is it impossible to argue that corporate directors breached his duty with gross negligence when he decided to introduce AIs to solve agendas that is too important (and widely considered to be relatively ill-AI-suited) to use unestablished technology ?

Some questions (cont'd)

About corporate governance structure: Is it correct to understand that the risk management committee in China is also acting as a committee for internal control and oversight? Also, is it correct to understand that the CTO in India is a senior executive primarily responsible for the execution of operations? My impression is that the executor tends to act as the accelerator and the auditor as the brake. How do CTOs (and, in that regard, CCOs) in India balance risk monitoring and execution? For example , if one board member recommends some data-providers (whose ability appears dubious and who might be bribing the said member), will CTOs be entitled to do the investigation to prevent conflict of interest, aside from analysing pros and cons of going into contract?





Thank you!