Digital trade rules and AI regulation – a primer

Jai Vipra, IT for Change
jai@itforchange.net

Highlights from this note:

- AI today affects most sectors of the economy and is primarily developed by Big Tech. Governments are yet to develop an adequate regulatory method for this sector;
- The proposed JSI on e-commerce restricts governments' ability to effective regulate AI, especially in terms of:
    - National security,
    - Prudential regulation, and
    - Economic value creation and value capture.
- Provisions not currently part of the JSI, but still under consideration, represent an even greater restriction on AI regulation, especially in terms of:
    - Data taxation
    - Regulation of cross-border data flows, and
    - Personal data protection;
- The moratorium on customs duties for electronic commerce could erode a significant portion of the revenue of importing countries as AI is used increasingly in products and services, and
- Multilateralism through consensus at the WTO is necessary for the inclusive and fair development of AI.

Recent developments in AI regulation

New developments in AI over the last year have created new opportunities as well as new risks. Governments worldwide have identified policy priorities in AI, including:

1. Algorithmic accountability, transparency, and standards: As AI models start making more decisions that affect the lives of people including workers, consumers, and public figures, questions of algorithmic accountability become critical. New legal provisions in different countries seek to institute transparency requirements for models and/or their development and deployment. Some sectoral standards also apply to AI models.
2. Liability: AI models, especially those employed in sensitive sectors like healthcare and education, may be subject to liability conditions that other software or humans in these sectors are subject to. Since AI models can often "hallucinate" (provide incorrect information), their inclusion even in less sensitive applications such as customer service must be carried out with a view to the cost of inaccuracy.
3. Governance of computational infrastructure: A complex supply chain of computation makes today's AI models possible. This includes chip design, manufacturing, assembly, testing and packaging. Governments have been paying an increasing amount of attention to the economic governance of computational markets.
4. Antitrust/competition policy: AI markets are extraordinarily concentrated. Vertical integration between cloud service providers, chip designers, AI model developers, and AI service providers is of particular concern. As AI is expected to affect a large number of industries, AI market concentration can have severe effects on the general concentration of wealth and power.
5. Data governance: AI models require a large amount of data for training and fine-tuning. Questions of personal data protection appear with renewed urgency, especially as Big Tech firms use data from their own products and services to train AI models. The value of non-personal data also becomes evident, as does the question of who captures this value.
6. Geopolitics and unequal development: Geopolitical rivalries dominate some parts of the AI policy sphere, especially on control over computational infrastructure. Countries in the Global South have particular concerns about unequal access to computational infrastructure and unfair global digital taxation regimes.
7. Misinformation and disinformation: AI models make it possible to generate mis- and disinformation at scale. Already, deepfakes have been used in election times and have affected various political and other public personalities. Vulnerable populations are at increased risk of targeting or even violence through disinformation.
8. AI-mediated unemployment: The widespread automation caused by AI in various sectors is likely to threaten many livelihoods. Unlike previous iterations of technology, there is little indication that AI will create more jobs than it replaces.
9. Environmental harms: Data centres that make AI possible require a tremendous amount of energy and water. Governments are interested in a cost-benefit analysis of AI products and the effect of their production on the environment.

Proposed trade rules that would impact AI regulation

At the WTO, trade rules being negotiated right now will have a lasting impact on governments' ability to regulate AI. Following are some issues with the negotiations on the Joint Statement Initiative (JSI) on E-commerce.

1. **Section B(2) Open government data**: Government data, like any other data, is a resource. It may be legitimate to use this data for public welfare. However, it is difficult to justify its use by Big Tech firms which do not share their own data as a resource. Data is a primary asset to improve the capabilities of AI models. Making government data available openly, especially at no or reasonable cost as the text stipulates, means disadvantaging the public sector and smaller firms in favour of larger firms. The provision in B(2)(7)(c) disallowing governments from restricting users from "(c) using the data for commercial and non-commercial purposes, including in the process of production of a new product or service." is particularly concerning. While the language of the provision is only that governments must "endeavour" to carry these activities out, such language can still represent an obligation. Governments must instead:
    a. Explore more controlled ways of sharing public data, especially with a view to creating competitive markets and avoiding capture by Big Tech, and
    b. Work on methods to develop mandatory sharing of non-personal data by firms who currently hold the largest amounts of such non-personal data.
2. Provisions that state, for instance, "for greater certainty, this Article is *without prejudice to a Party's laws* pertaining to intellectual property and personal data protection", or "this Article applies to measures by a Party with respect to data held by the central government, *disclosure of which is not restricted under domestic law*" are still insufficient to ensure that governments can make their own laws in regards to data. This is because it is unclear at what time such laws must already have been in place for them to not contravene the agreement, and if laws made in the future are exempt.
3. **Section A(2)(3) Electronic authentication and electronic signatures**: This provision deregulates the security of electronic transactions, disallowing the government from making rules for commercial transactions. With the increasing use of AI in authentication, there are specific cybersecurity and fraud risks that arise due to model hallucinations and other shortcomings. Governments must retain their existing powers to regulate authentication and electronic transactions as they see fit. The agreement text does not allow governments enough leeway to do so – laws and rules must already be in place to be legitimate. Provisions in A(2)(4) are not sufficient because governments may require more than standards or certification for authentication.
4. **Scope and general provisions (7)(2) Prudential exceptions**: While the provision allows governments to ignore the agreement for prudential regulation, this subsection makes that power too contingent. If measures that do not meet obligations in the agreement cannot be used to avoid obligations in the agreement, they are not really exceptions. As discussed above,

prudential regulation with the use of AI in finance might be particularly important[1] and a more explicit carveout is necessary.

5. **Scope and general provisions (6) Security exception:** The agreement adopts the same security exceptions as Article XXI of the GATT 1994 and Article XIV *bis* of the GATS. This exception is extremely limited. The exception applies only to fissionable and fusionable materials, supplying military establishments with arms, ammunition and services, and wartime policymaking. The use of AI in military applications is now rampant and not just in wartime. Additionally, security considerations are also important when AI is used to run or compromise critical public infrastructure. Instead of being limited by this stringent constraint, governments worldwide must have the ability to regulate the use of AI in defence in the public interest, as well as to enter agreements to prevent cascading and catastrophic consequences from the use of AI in such applications. In general, the sovereignty of a country in determining the use of technology in defence applications must not be limited by trade agreements.

Other issues in digital trade for AI regulation

1. **Free cross-border data flows**: Provisions banning governments from adding conditions to cross-border data transfers have been part of earlier drafts of the JSI e-commerce agreement. Such provisions would be disastrous for governments' ability to protect their citizens' personal data, tax data adequately, and meet national security obligations. The effect of these restrictions on antitrust options would also be significant, since the separation of data resources from computational resources and model development could form a core of antitrust policy in some countries. They would also threaten national competitiveness in AI development, as some countries with more AI preparedness in terms of computational infrastructure would be able to freely exploit other countries' relative competitiveness in data, and thus develop superior AI models.
2. **Restrictions on source code disclosures**: Any provision that would ban governments from requiring disclosure of "source codes" broadly defined would threaten algorithmic accountability, transparency and standards. The widespread use of AI in all sectors means that such a provision cannot stand muster in practical terms.
3. **E-commerce moratorium**: Renewing or making permanent the moratorium on customs duties on electronic transmissions would erode a significant revenue base of many countries in an age where not just services, but also products, have a digital component. Any product or service that contained an AI component, for instance, could evade customs duties for that component. Given that much of the value of such products now accrues to the digital component, this evasion represents a significant loss for countries that import these products. Already, an analysis by South Centre's Rashmi Banga shows that between

[1] Consider a situation where algorithmic investment through widely used automated advisors or brokers leads to a cyclical disinvestment problem, causing macro-prudential issues. Financial regulators would require the freedom to regulate such that these situations do not occur and macroeconomic stability is not threatened.

2017-2020, developing countries and LDCs lost tariff revenue worth $56 billion due to the e-commerce moratorium being in place. It is therefore not advisable to renew the e-commerce moratorium under current conditions.

Conclusions

1. An agreement on the digital aspects of trade is important, but if it is not arrived at through true multilateral consensus, significant issues of concern to many countries, such as those outlined above, will be missed. The process to develop such an agreement must be carried out not through a JSI, but through the usual process of negotiation at the WTO.
2. AI today is dominated by Big Tech; regulating this sector is a priority for several countries. No country has yet developed an adequate regulatory package to tackle the impact of this sector on the global economy and society in general. A premature and restrictive agreement that goes beyond its mandate of trade can hamper countries' abilities to find new and creative ways to appropriately regulate this sector in the public interest.

Acknowledgements

This brief was written based on in-depth analyses of negotiations and agreement texts of several researchers, primarily Jane Kelsey, Sanya Reid Smith, Parminder Jeet Singh, Deborah James and Richard Hill.