RCEP's Contribution to Global Data Governance

By:

Thomas Streinz

February 19, 2021

Data has emerged as a major topic in global governance. The forthcoming World Development Report hails data's potential for economic development. The COVID-19 pandemic exposed how rapidly economies may shift towards different configurations, facilitated by and dependent on platforms that rely on the Internet's data transfer infrastructure. Access to and control over data promises superior economic performance and is crucial for the development and deployment of machine-learning algorithms. Despite its potential for non-rivalrous dissemination and consumption, data has become a contested economic resource. Polities and publics around the world are grappling with the immense economic, social, and political transformations that datafication and constant digital inter-connectedness entail. They ought to confront immense power imbalances across and within countries as well as between gigantic technology corporations, largely headquartered in the US and China, and businesses and consumers who have come to rely on their infrastructures. North-Atlantic critiques of "surveillance capitalism" all too easily overlook the continuities, similarities, and even path dependencies that link today's data

capitalism to pre-digital imperialism, colonialism, and extractivism. From a "Global South" perspective, questions of data inequality and AI justice look all too familiar.

As the debate around global data governance gains traction and data geopolitics take shape, the relevance of existing and emerging frameworks of international economic law for global data governance remains underappreciated. The beleaguered World Trade Organization (WTO) remains ostensibly the institutional center for international trade law and plurilateral negotiations for new rules on "electronic commerce" are ongoing, but a consensus is likely to remain elusive. Countries have made highly uneven commitments under the General Agreement on Trade in Services (GATS) and their constraining force against restrictive data policies has hardly been tested within the WTO's dispute settlement system. Instead, the global tech industry has lobbied for new rules in increasingly "comprehensive" trade and investment agreements.

These efforts are often portrayed and defended as new rules on "electronic commerce" and "digital trade" but their conceptual, economic, and political nexus to conventional trade and investment law is tenuous. Instead of understanding these provisions as mere "updates" to international trade and investment law, they might be better understood as part of a "megaregulatory" agenda. Digital megegaregulatory agreements determine the conditions under which countries may craft their domestic data governance regimes and shape frameworks for global data governance.

The Regional Comprehensive and Economic Partnership (RCEP) agreement between the ten ASEAN countries and their dialogue partners—China, Japan, South Korea, Australia, and New Zealand—created a modified template for international data governance. It marks a new attempt to reconcile the technological potential and economic rationale for digital inter-connectivity with countries' ability to regulate their increasingly digital economies and societies.

Before RCEP, the debate was often perceived and portrayed as a transatlantic power struggle between the US and the EU, with everyone else either aligning themselves or refraining from crafting data governance provisions into international economic agreements altogether.

The United States inaugurated a new model for rules on the digital economy during the Obama-era negotiations for the Trans-Pacific Partnership (TPP). The key provisions concern requirements to use domestic computing facilities and cross-border data transfer restrictions as two archetypes of "data localization". The TPP model has been remarkably influential despite the US withdrawal from TPP. The remaining eleven parties retained it in the revived CPTPP. The US negotiated a sharper version into its new NAFTA with Canada and Mexico and its "digital trade" agreement with Japan (eliminating justifications for requirements to use local computing facilities). The Digital Economy Partnership Agreement (DEPA) between Chile, Singapore, and New Zealand, in force for the latter two since 7 January 2021, reaffirms these countries' commitment to the TPP model. The same is true for the Australia-Singapore digital economy agreement. The countries that sign on to these provisions adhere to the Silicon Valley Consensus, according to which "free" data flows are essential to economic growth and prosperity. Regulatory interventions that limit data mobility need to satisfy meta-regulatory rules that prohibit arbitrary and unjustifiably discriminatory measures and disguised restrictions on trade. Crucially, measures must not exceed what is necessary to achieve their objective, thereby subjecting data policies to a means-ends test that invites external second-guessing and scrutiny.

The EU has resisted such constraints and instead cast itself as a regulatory superpower in the digital domain, championing data protection and privacy as fundamental rights. Its General Data Protection Regulation (GDPR) has been widely portrayed as a model to be emulated if not replicated. However, the GDPR's restrictive regime for transfers of personal data to third countries has complicated transatlantic data relations, as the EU's Court of Justice twice annulled the relevant arrangements at the behest of privacy activist Max Schrems, first Safe Harbour, then Privacy Shield. The US model, as created for TPP and replicated elsewhere, would constrain the EU's data transfer regime by asking whether the European Commission's adequacy assessments satisfy standards of non-arbitrariness and non-discrimination and whether it is truly "necessary" to have general restrictions on cross-border transfers of personal data to begin with. The EU has not been keen on such inquiries. Its model for data governance in EU trade and investment agreements protects its data protection regime from external scrutiny and only bans the kinds of data

localization that the EU itself is not engaged in. Requirements to store or process data within a country's territory are being outlawed, but cross-border data transfer restrictions remain unscathed.

RCEP echoes TPP's and other agreements' commitment to data mobility as a new objective of international economic law (irrespective of corresponding trade and investment flows). RCEP ostensibly uses TPP as its blueprint but modifies it in a way that retains countries' ability to craft restrictive data policies when they deem it necessary. The principal recognition that Parties may employ different data localization measures is quickly followed by a principal prohibition of such measures, which is then cabined by the possibility to justify them under certain conditions. To put this into rule/exception terms: the rule is to not require the use of domestic computing facilities or to restrict the cross-border transfer of information. Exceptionally, such measures may be deployed under certain conditions. It is in this regard that RCEP deviates from TPP. Under TPP, parties need to show that their measures pursue a legitimate public policy objective and are not arbitrary, unjustifiably discriminatory, or a disguised restriction on trade, and that the restrictions are not greater than necessary. If need be, these questions could get adjudicated in state-state dispute settlement proceedings. In contrast, under RCEP, it is for each country itself to decide what "it considers necessary" to achieve a legitimate public policy objective. As a footnote makes clear, "the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party". Other Parties may only allege that a measure is arbitrary, unjustifiably discriminatory, or a disguised restriction on trade but they cannot claim that it does not pursue a legitimate public policy objective or that it is not necessary. Parties retain even greater leeway with regard to measures they consider necessary for the protection of "essential security interests". Such measures are protected from other parties' scrutiny altogether. In contrast to TPP, RCEP does not foresee the use of state-state dispute settlement for data governance commitments (but it does contemplate that this could get revisited upon review of the agreement, in which case Parties may opt-in into state-state dispute settlement). Instead, RCEP encourages good faith consultations between the Parties and within RCEP's Joint Committee.

On other data governance issues, parallels between TPP and RCEP are more pronounced. RCEP mimics TPP in letting the mere existence of any kind of data protection and privacy framework suffice (Cambodia, Laos, and Myanmar have five years to create one). As in TPP, protection of personal information is seen as desirable for economic reasons, not out of a principal commitment to data protection and privacy as human rights. The requirement to publish the relevant data protection laws is a welcome contribution to comparative data protection law scholarship and practice. RCEP even includes an entirely new provision, which continues the trend towards business conduct regulation in international economic law, that requires parties to encourage companies to publish their privacy policies. The RCEP countries commit to take evolving global data protection standards into account, but do not explicitly reference any, including the APEC Privacy Framework.

To assess RCEP's contribution to global data governance, it is instructive to look at the new template from the perspectives of China, which is a party to RCEP, India, which participated in the negotiations but did not sign the result, and other third countries currently contemplating the inclusion of data governance provisions into their international economic agreements. If held against TPP as a benchmark, RCEP may either seem less constraining or less ambitious, depending on one's normative disposition.

That RCEP's electronic commerce chapter contained binding data governance provisions at all marks the first time that China has entered into such commitments. China's previous trade and investment agreements only included e-commerce chapters with only perfunctory language (if at all). When the US sought to cast TPP as a check on China, it sometimes pointed to TPP's data governance provisions as fundamentally incompatible with China's data localization requirements. RCEP is the first indication of what kind of data governance provisions China is willing to accept. RCEP combines a principal commitment to data mobility with very broad carve outs that reduce the risk of external challenges to internal data governance policies to a minimum. The broad security carve out, in particular, allows China to retain its restrictive data governance regime without external scrutiny.

India has not signed any trade and investment agreement with binding data governance provisions. Its vociferous opposition against the WTO's efforts in

this domain are well known. While this position has roots in long standing trade disputes, it also coincides with India's experiment of crafting openly protectionist data governance policies as an economic development strategy. In theory, one could defend such policies under RCEP's permissive regime, but in reality, the conceptual and ideological tensions might be too strong.

The treaty language on data governance that RCEP pioneered is likely to appear in future agreements whenever countries seek to combine a principal commitment to data mobility with largely unconstrained regulatory freedom. Whether this balance or abstaining from data governance provisions in international economic agreements altogether is desirable, depends on each country's economic, social, and political calculus. Sound policy making is greatly inhibited by the dearth of data about data control, data flows, and data value, a problem that various International Organizations are trying hard to address. Smaller countries, in particular, might be better off by banding together instead of crafting independent data governance policies.

While RCEP creates a modified data governance template, it remains within the logic of 20th century treaty language and design. Meanwhile, a normative reevaluation of international economic law is overdue and ongoing. Depending on whether international economic law's arc will continue to bend towards economic efficiency and aggregate welfare gains rather than planetary environmental sustainability, individual human flourishing, and justice, future international economic law may need to change in form and substance. To make treaties data-ready for the 21st century, more dynamism, flexibility, and experimentation are desirable. Privacy advocates and Internet activists, who often view trade negotiations as illegitimate vehicles for global data governance and decry the departure from multistakeholder configurations and norms common in Internet governance settings, can play a constructive role in pushing these broader conversations forward.

View online: RCEP's Contribution to Global Data Governance

Provided by Afronomicslaw