

Encyclopedia of International Economic Law

Edited by Prof. Krista Nadakavukaren Schefer and Prof. Thomas Cottier

Privacy and data protection in trade agreements

Mira Burri

Against the backdrop of the advanced digitization of world trade and the serious implications of the data-driven economy for the protection of personal data, the topic of privacy and data protection has become a central element in policy debates during trade negotiations. It has also been reflected in the latest generation of trade treaties of bilateral and regional nature that seek to reconcile the free flow of data, as a fundament for the seamless data economy, and the protection of the right to privacy.¹

Privacy under the WTO framework

Privacy and data protection were not discussed during the Uruguay Round. Although the WTO membership recognized the implications of digitization for trade already in 1998, launching a Work Programme on E-commerce, this initiative to revise the rules in the domains of trade in services, trade in goods, intellectual property protection and economic development did not bear any fruit over two decades. WTO law nonetheless applies to online trade, as many of the existing rules and commitments are technologically neutral and can be applied to online situations, as confirmed by GATS cases. WTO law also includes certain mechanisms, such as the ‘general exceptions’ formulated under Article XX GATT 1994 and Article XIV GATS, that are meant to reconcile economic and non-economic objectives and domestic values such as privacy protection. Of specific interest for this contribution’s discussion is the extent to which the general exceptions can be used to justify maintaining and adopting restrictions to trade on the grounds of privacy protection. While Article XX GATT does not provide a fitting category, Article XIV GATS does. Article XIV(c)(ii) GATS specifies that laws and regulations related to ‘the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts’ can be ‘excused’. The application of this exception has not been tested so far but there is scholarly literature that has discussed it. The focus has been in particular on exploring whether the high standards of protection endorsed by the European Union (EU)’s General Data Protection Regulation (GDPR) would pass the test of the GATS exception clause.² Some doubts as to the compatibility of the GDPR have been expressed in this regard, as the EU might not find appropriate evidence on the performance of the GDPR, which would undermine the strength of a challenged measure’s contribution to securing compliance. Another argument put forward is that there might be less trade restrictive measures reasonably available for attaining the EU’s desired level of data protection, as the GDPR is in many respects excessively burdensome with sizeable extraterritorial effects. Thirdly, the GDPR provisions on the transfer of personal data to third countries could fail the chapeau test of Article XIV GATS, as the EU might not have been consistently implementing them, discriminating between different countries in finding adequate levels of protection and in cooperating with them.³

Beyond the general exceptions in WTO law, finding a balance between data protection at home and the liberalization of digital trade and cross-border data flows in particular has become a

¹ M. Burri, ‘Interfacing Privacy and Trade’, *Case Western Journal of International Law* 53 (2021), 35–88; A. Chander and P.M. Schwartz, ‘Privacy and/or Trade’, *University of Chicago Law Review* 90 (2023), 49–135.

² See R.H. Weber, ‘Regulatory Autonomy and Privacy Standards under the GATS’, *Asian Journal of WTO and International Health Law and Policy* 7 (2012), 25–47; K. Irion, S. Yakovleva and M. Bartl, *Trade and Privacy: Complicated Bedfellows?* (Amsterdam: Institute for Information Law, 2016), at 27–33.

³ Irion et al., *ibid.*, at 36–39; also D.A. MacDonald and C.M. Streatfeild, ‘Personal Data Privacy and the WTO’, *Houston Journal of International Law* 36 (2014), 625–652, at 640–650.

critical topic under the currently negotiated Joint Initiative (JI) that seeks the adoption of a plurilateral agreement on electronic commerce under the umbrella of the WTO. The scope and contents of such an agreement are to a large extent shaped by the developments in preferential trade forums, discussed in the next section.

Privacy and data protection in FTAs

As the WTO has not directly responded to the digital transformation of economies,⁴ states have used FTAs to increasingly regulate different aspects of digital trade. Out of the 384 agreements signed between 2000 and 2022, 167 contain provisions on digital trade and 109 have dedicated digital trade chapters.⁵ The latter, together with a new type of treaties – the so-called ‘Digital Economy Agreements’ – have become a critical source of new rule-making that goes beyond conventional trade law’s aspirations to reduce trade barriers and liberalize economic sectors. The new rules differ in their aims and can be clustered into two categories: (1) rules that seek to facilitate digital trade, covering for instance electronic contracts, electronic signatures, and paperless trading; and (2) data governance rules.

The latter category of data governance provisions, which cover cross-border data flows, data localization measures and personal data protection are the ones pertinent for this contribution and have been among the most contentious issues in trade negotiations. They are also the source of observed divergences among stakeholders (with marked disparities between the United States [US], the EU and China), as they share different stances on the interfaces between trade commitments, domestic regulatory regimes, and the protection of privacy under these regimes.

In the era of Big Data, there has been a widely shared acknowledgment that the right to personal data protection is particularly affected by to pervasive data collection and use by both companies and governments. In the national context, this acknowledgement triggered the reform of data protection laws around the world, best exemplified by the EU GDPR. In the trade law context, an increasing number of FTAs prescribe the adoption of data protection frameworks and compliance with existing international standards. However, as privacy protection has been regulated differently across countries, with important variations even between constitutional democracies such as the US and the EU, the approaches in digital trade law, too, have been divergent. The EU endorses personal data protection as a fundamental right and ensures a host of safeguards in place to protect its policy space. This includes a provision on data sovereignty; and a clause that permits adjustments to data commitments after the treaty’s entry into force; as well as a broadly-defined ‘right to regulate’, which covers anything from personal data protection to cultural diversity as a ground for limiting data flows. In contrast, the US and a number of countries in the Asian Pacific region, such as the those that are parties to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States–Mexico–Canada Agreement (USMCA), have chosen to prioritize trade over privacy and only adopted softer provisions on personal data protection.

These divergences translate into differential FTA rules on data flows. Under the US model, which has been followed in a number of other treaties, cross-border flows of data, including personal information, must be allowed and no data localization measures are permitted. So, for instance, the CPTPP explicitly prohibits the parties from requiring a ‘covered person to use or locate computing facilities in that party’s territory as a condition for conducting business in that territory’ (Article 14.13(2)). The soft language on free data flows found in the US–Korea FTA is framed as a hard rule: ‘[e]ach Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person’ (Article 14.11(2)). Measures restricting digital data flows or localization requirements are permitted only if they do not amount to ‘arbitrary or unjustifiable discrimination or a disguised restriction on trade’ and do not ‘impose restrictions on transfers of

⁴ M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021); S. Peng, C. Lin and T. Streinz (eds), *Artificial Intelligence and International Economic Law* (Cambridge: Cambridge University Press, 2021).

⁵ This analysis is based on the TAPED dataset administered by the University of Lucerne. For all data, see <https://unilu.ch/taped>.

information greater than are required to achieve the objective' (Article 14.11(3)). These non-discriminatory conditions are similar to the test formulated by Article XIV GATS and Article XX GATT 1994 but differ from the WTO exceptions in that they apply to any 'legitimate public policy objective', not just to the objectives enumerated in the WTO general exceptions (Article 14.11(3) CPTPP). Other treaties, such as the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore, have chosen another approach in terms of reconciliation mechanism and simply restate the texts of Article XIV GATS and Article XX GATT 1994 and parties pledge to apply them *mutatis mutandis*.

Under the EU model, the regime is conditional, and data can flow only if certain requirements, notably compliance with the high standards of the GDPR, are satisfied – as testified to by the recent trade deals of the EU with the United Kingdom and New Zealand. For reasons that have to do less with the protection of fundamental rights, China too applies a conditional, albeit much more stringent and opaque regime, as seen from the Regional Comprehensive Economic Agreement (RCEP) to which China is a party.

Concluding remarks and outlook

The data-driven economy has ushered in new challenges for trade law. It has also added new important topics to trade negotiations and rule-making that demand a proper interfacing of economic and non-economic objectives. The domain of data protection appears to be the most pertinent in this context, as governments seek to provide adequate protection of the privacy of their citizens while at the same time enable cross-border data flows as an essential element for data-driven growth and innovation. The next years will show to what extent international cooperation in digital trade regulation will bring about viable models that can ensure this balance – under the umbrella of the WTO, in the framework of preferential trade agreements or in discrete treaties, such as the Digital Economy Agreements. In this context, it has also been discussed whether there is a need to provide for minimum standards of privacy protection at the international level that can also provide useful references for trade forums.⁶ Others have argued in contrast that data privacy should not be put in trade law at all.⁷

Key literature:

M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021).

M. Burri, 'Interfacing Privacy and Trade', *Case Western Journal of International Law* 53 (2021), 35–88.

M. Burri, 'Privacy and Data Protection', in D. Bethlehem, D. McRae, R. Neufeld and I. Van Damme (eds) *The Oxford Handbook on International Trade Law*, 2nd edn. (Oxford: Oxford University Press, 2022), 745–767.

A. Chander and P.M. Schwartz, 'Privacy and/or Trade', *University of Chicago Law Review* 90 (2023), 49–135.

S. Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy', *University of Miami Law Review* 74 (2020), 416–519.

⁶ Chander and Schwartz, above note 1.

⁷ Kristina Irion, Margot E. Kaminski & Svetlana Yakovleva, 'Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law', *University of Chicago Law Review Online* (2023); S. Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy', *University of Miami Law Review* 74 (2020), 416–519.