Governing cross-border data flows

Reconciling EU data protection and international trade law

Yakovleva, S.

Publication date
2021

6. Conclusions

This thesis has tackled the timely issue of reconciling the governance of cross-border data flows from the perspectives of EU data privacy protection and international trade law. It has demonstrated a real clash between international trade and European data privacy law when it comes to the governance of cross-border flows of personal data. This clash is the result of the coming together of a multitude of factors. Among them, the following three are of particular importance: (a) the pivotal importance of personal data in digital commerce; (b) the increased level of protection of the rights to privacy and the protection of personal data since 2009 as binding fundamental rights under the EU Charter; and (c) the recent trend of governing cross-border data flows by regional, plurilateral and multilateral trade agreements.

This thesis has provided the necessary background and analysis of EU rules governing cross-border transfers of personal data in the light of the EU Charter and the ways in which this issue is addressed in the current and proposed trade agreements led by the EU and the US. It also put the developments in both areas against the background of EU constitutionalisation and trade policy. In order to resolve the tensions caused by the above-mentioned clash, this thesis has analysed and proposed ways to ameliorate the situation from both ends (trade and personal data protection), specifically through reforms of both international trade rules in future trade agreements and GDPR rules. To explain how such reforms could be effectuated, the thesis has also aimed to fill in a significant lacuna in existing literature by looking at the role of discourse in the evolution of trade law, in particular in its relation to cross-border data flows. In doing so, the thesis considered the digital trade discourses currently advanced by the EU and the US in the course of negotiations of digital trade agreements, revolving around the issue of whether, and to what extent, restrictions on cross-border data flows amount to 'digital protectionism'. The thesis has shown the importance of discourse in any attempt to reform trade rules.

This thesis answered the following research question:

> *how should commitments on cross-border data flows in future EU trade agreements be reconciled with the protection of the fundamental rights to privacy and personal data?*

In answering this research question, this thesis has concluded that, in order to reconcile cross-border data flows with data protection and privacy without undermining fundamental rights, a reform of trade law rules in the EU's future trade agreements and the GDPR rules on transfers of personal data outside the EEA is necessary. Tackling each of the research sub-questions specifically, the thesis has made the following propositions.

1. Simultaneous application of international trade and EU Charter rules to the restrictions on transfers of personal data outside the EEA may create a catch-22 compliance deadlock for the EU. On the one hand, there is a risk of inconsistency between the obligation on cross-border personal data flows, which can be deduced from the EU's commitments under the GATS in the context of digitally provided services, and the restrictions on transfers of personal data under the GDPR. This inconsistency may not be justifiable under the general exception for privacy and data protection in trade agreements. On the other hand, from an EU Charter perspective, the level of liberalisation of cross-border data flows required by the GATS constitutes an interference with the fundamental rights to privacy and the protection of personal data under the EU Charter. This interference may not be justifiable under Article 52(1) of the Charter.

Although the GATS does not specifically regulate cross-border data flows, in Section 2.2 the thesis concludes that the different treatment of transfers of personal data outside the EEA to countries that have been an granted adequacy decision, and other countries, could be in violation of the MFN clause contained in the GATS. Similarly, the different treatment of personal data transfers to companies that have an establishment in the EEA compared to those who do not could result in a violation of the national treatment. The 2020 *Schrems II* judgement of the CJEU puts more pressure on the GDPR's framework for transfers of personal data from an international trade perspective. In particular, the (soft) data localisation, that could follow in the aftermath of the judgement allows for the interpretation of this CJEU judgement as a violation of the EU's market access commitments.

Next, Section 2.3 concludes that the scope of the general exception contained in GATS Article XIV(c)(ii) – perhaps the most important legal mechanism to accommodate the EU's autonomy to adopt and maintain rules that would otherwise be inconsistent with its GATS commitments – may not be broad enough to justify the EU's restrictions on transfers of personal data outside the EEA. The main reason for that insufficiency is that these restrictions are unlikely to pass the necessity test (referred to as the 'trade necessity test' in this thesis), which lies at the core of this exception. The trade necessity test requires, in particular, that a GATS-inconsistent trade-restrictive measure be the least trade restrictive of all reasonably available measures to achieve the level of protection of the public interest at stake. Relying on existing WTO case law, the thesis concludes that there are at least two reasons for the tension.

First, within the 'range of degrees of necessity' in WTO caselaw, the nexus between the existing EU framework for transfers of personal data – specifically the adequacy requirement – and the underlying purpose of ensuring a high level of protection of personal

data, is closer to 'making a contribution' rather than 'indispensable'. The sizeable gap between what the EU framework for transfers of personal data outside the EEA *should* and *can* deliver makes it far from clear that it would pass the necessity test of the general exception in trade agreements.

Second, the EU's restrictions on transfers of personal data are among the most restrictive in the world. Against the backdrop of the weaknesses that the EU framework for transfers of personal data contains (elaborated upon in greater detail in Section 5.3), one could argue that other approaches to personal data transfers could be 'reasonably available' to the EU to achieve the same level of protection. Such other approaches could, for example, include the OECD and the APEC frameworks or the framework codified in Convention 108+. This argument is, however, only valid if the *same* level of protection is viewed as that *actually achieved* by the current framework as opposed to the *desired* level of protection in the light of the EU Charter.

The thesis then flips the analysis by looking at it from the perspective of the EU Charter, which requires that rules, including international agreements and interfering with the fundamental rights to privacy and the protection of personal data, should be least restrictive of such rights. While international trade law starts from the premise that cross-border data flows should be allowed, the EU Charter instead posits that those data flows outside the EEA should be conditionally restricted. As a result, should a WTO adjudicating body find EU restrictions inconsistent with the GATS and unable to be justified under the general exception, compliance with such a decision could be inconsistent with the necessity test under Article 52(1) of the EU Charter. This provision sets constitutional limits on the extent to which the EU institutions can derogate from the fundamental rights, including the rights to privacy and the protection of personal data. Although the EU Charter does not establish any hierarchy between fundamental rights, in a line of cases (that includes most notably *Volker und Markus Schecke, Digital Rights Ireland, Tele 2, Schrems I, Opinion on EU-Canada PNR Agreement* and, most recently, *Schrems II*), the CJEU has elevated the EU Charter necessity test to the level of 'strict necessity' in relation to derogations from the fundamental rights to privacy and the protection of personal data. Relaxing restrictions on transfers of personal data to the extent consistent with the requirement of being the least trade restrictive is unlikely to pass the strict necessity test under the EU Charter. In other words, international trade obligations governing cross-border data flows may require the EU to derogate from these fundamental rights further than it is allowed within its own constitutional boundaries. Facing the choice of violating its trade obligations or the EU Charter, the EU may find itself in a catch-22 compliance deadlock.

Although in the hierarchy of EU law, the EU Charter, as primary EU law, is situated above international trade agreements, this does not make international trade law less binding on the EU. From an international law perspective, the EU must perform its

international trade obligations in good faith and may face liability and retaliation for failing to do so. This is why constitutional restrictions on compliance with trade obligations or decisions of trade adjudicating bodies could present a serious problem, especially in the context of international trade negotiations of future trade agreements, for at least two reasons. First, the TFEU requires that in the course of international trade negotiations the EU institutions must ensure compatibility of any trade agreements with the internal EU policies and rules. Failure to do so may result in a CJEU judgement under Article 218(11) TFEU, finding that a prospective trade agreement is inconsistent with the EU *acquis* and ultimately requiring EU institutions to renegotiate a (part) of the agreement. Second, the EU's rhetoric in trade policy discourse, which is that personal data and privacy cannot be traded, is an important internal political message. An attempt to negotiate an exception for privacy and data protection that could potentially undermine the EU's domestic framework safeguarding such protection is likely to be opposed by the European Parliament, both during the negotiations and the actual legislative process. Therefore, to alleviate the possible tension between the trade and EU Charter necessity tests, this thesis has concluded that, from a trade law perspective, the EU's future trade agreements containing more elaborate provisions governing cross-border data flows *should not* replicate the general exception for privacy and data protection from GATS Article XIV.

2. It is not possible to strike the right balance between domestic data privacy protection and liberalisation of digital trade by just ruling out 'protectionism'. Where the line should be drawn between legitimate protection and protectionism is strongly influenced by the discourse governing policy conversations on domestic privacy and the protection of personal data in the context of international trade. Therefore it is crucial for the EU to frame future digital trade negotiations in terms of pluralist – as opposed to purely economic – discourse. Under the narrow, effects-based definition of 'protectionism' generated by neoliberal discourse on international trade, EU restrictions on transfers of personal data outside the EEA can be viewed as protectionist. A broader, pluralist discourse is necessary to allow the EU to strike the right balance between globalisation, democratic politics, and the domestic autonomy to pursue domestic values such as the fundamental rights to privacy and data protection.

Before diving into the discussion of the ways in which to reform the exception for privacy and data protection in future trade agreements in Chapter 4, in Chapter 3 the thesis takes a step back and offers a bird's eye perspective on the dynamics of international trade reforms through trade negotiations and the interpretation of trade rules by adjudicating bodies. Informed by established methods of discourse analysis, Section 3.2 demonstrates the role of discourse in the redefinition of 'protectionism' in trade negotiations and in the interpretation of trade rules throughout the history of the development of the international

trading system. It explicates that the term 'protectionism' is not endowed with a specific meaning, and shows that its definition is, to a large extent, a product of discourse. Against this backdrop, Section 3.3 juxtaposes the digital trade discourses of the EU and the US and shows how the meaning of what these trading partners label as 'digital protectionism' differs depending on the values underlying each discourse. Using the economics-based 'digital trade' discourse advanced by the US, this section demonstrates how 'digital protectionism' and similar terms that are often used to label restrictive data protection regimes, trigger a fundamental redefinition of what constitutes a barrier to trade and, thus, pushes towards deeper trade liberalisation and favours the deregulation of personal data transfers. Furthermore, Section 3.4 of the thesis concludes that the value structures attending the discourse ultimately predetermine where the line will be drawn between legitimate privacy and personal data protection, and illegitimate protectionism – both in the relevant provisions of international trade agreements and in the interpretation of such provisions by trade adjudicating bodies. Exposing the limitations of the dominant economic discourse when it comes to protection of privacy and personal data as fundamental rights, the thesis highlights the importance for the EU of maintaining a pluralist discourse.

Ultimately, the *definitional* distinction between privacy and personal data protection and protectionism is in part a *moral* question, that is, it should not be viewed just as a question of economic efficiency. Therefore, when a policy conversation, such as the one on cross-border flows of personal data, involves non-economic spill-over effects to individual rights, such conversation should not be confined within the straightjacket of trade economics, but rather placed in a broader normative perspective.

From a global perspective, the thesis concludes that a consensus on discourse and its underlying values is likely to be essential for the success of ongoing multilateral trade negotiations. This discourse should be defined on the basis of the goals of international trade for the twenty-first century and how far domestic regimes are willing to let trade rules interfere in their autonomy to protect their societal, cultural and political values. What actually constitutes 'protectionism' should be defined based on the outcome of this discussion.

3. The trade law model clauses on cross-border data flows and the protection of personal data and privacy proposed by the EU do not allow the EU to strike the right balance between fundamental rights protection and the EU digital trade policy objectives. These clauses, however, do allow the EU to fully safeguard its autonomy to protect privacy and personal data as fundamental rights. They also send a clear message to the public about the EU's commitment to do so. Nevertheless, these clauses are unlikely to fulfil the EU's ambition to liberalise the flows of data *into* the EU and

maintain a multilateral rules-based trading system. One of important ways to improve the clauses is to replace the threshold 'it deems appropriate', contained in the proposed exception for privacy and data protection, with a standard of non-circumvention, non-avoidance or reasonableness. When implemented in trade agreements, these standards should be complemented by restrictive mechanisms imposing checks and balances on trade adjudicators' powers of interpretation.

As this thesis concludes in Chapter 2, the exception for privacy and data protection in the EU's future trade agreements requires a lower threshold than the necessity test in the GATS general exception. In an attempt to design such a new exception, in 2018 the EU proposed model clauses for its prospective digital trade agreements, which included a provision on cross-border data flows and an exception for the protection of privacy and personal data (the 'digital trade exception'). These clauses are a part of the current EU's digital trade policy aiming, in particular, at removing 'protectionist' restrictions on cross-border data flows from other countries into the EU. As a part of its general trade policy, the EU promotes multilateralism and a rules-based global trading system.

The provision on cross-border data flows prohibits an enumerated list of restrictions on such flows. None of these prohibitions is likely to affect the EU's own restrictions on transfers of personal data outside the EEA under the GDPR. The digital trade exception includes a subjective 'it deems appropriate' test – modelled after the 'it considers necessary' test of the national security exceptions in the WTO Agreements (for example, Article XXI GATT and Article XIV*bis* GATS). That is the broadest of all current exceptions in international trade law. If one were to put the trade necessity test and the 'it deems appropriate' test on a continuum, from most restrictive to least restrictive thresholds for domestic autonomy in international trade, they would be at the opposite ends of such a continuum.

Chapter 4 of this thesis concludes that the proposed model clauses suffer from at least three weaknesses and should be improved. As a result, they do not allow the EU to reconcile fundamental rights protection with its digital trade policy, while promoting a rules-based trading system. First, the material scope of the proposed digital trade exception is uncertain due to unclear relationship between this exception and the general exception for privacy and data protection, which is simultaneously included in the EU proposals for trade agreements. The best way to address this concern would be to replace the two separate exceptions with a consolidated one that would apply throughout the trade agreement. However, this may be hard to achieve in practice due to the high costs of renegotiating the general exception, and its 'legacy clout'. Therefore, as a minimum, the relationship between the two exceptions should be clarified.

Second, modelling the threshold for the proposed digital trade exception on the national security exception is undesirable. Because the prohibitions on cross-border data flows are targeted at the EU's trading partners, it is these partners – and not the EU itself – who are most likely to invoke the digital trade exception. The breadth of the 'it deems appropriate' threshold, on which this exception is based, can justify almost any derogation from a prohibition of restrictions on data flows. As a result, it may undermine the EU's trade policy objective of removing restrictions on cross-border data flows *abroad*. In addition, including such a low threshold (until now reserved only for national security interests that are vital for any state) in an exception for privacy and data protection, on the one hand, puts the latter policy objectives on par with national security and above other policy objectives that still fall under the general exception (for example, public health). This creates an incentive to frame a broader set of policy objectives as privacy and data protection to escape international trade law disciplines. On the other hand, this also opens the door for using the same low threshold in other exceptions in the future. Ultimately, including such a low threshold in the digital trade exception may contribute to further undermining of the international rules-based trading system. Therefore, the proposed digital trade exception should be based on a different threshold – somewhere in between an overly broad 'it deems appropriate' test, and an overly restrictive 'necessity' test.

Based on an in-depth analysis of academic literature and the WTO case law concerning other thresholds used in WTO agreements to balance trade liberalisation against other public policy objectives, Chapter 4 of this thesis concludes that a 'non-circumvention', 'non-avoidance', or 'reasonableness' threshold would be a better option than the 'it deems appropriate' threshold proposed in the digital trade exception. All of these thresholds are interpreted by recourse to the *principle of good faith and the prohibition of abuse of right*, which preserves the flexibility of the 'it deems appropriate' test but acts as a counterweight to the almost unrestricted nature of the latter. To control for the drawbacks that come with the flexibility of those principles, the use of any of these thresholds should be complemented by restrictive mechanisms, such as institutional controls already implemented in the Understanding on the interpretation of the prudential carve-out in CETA. In particular, this mechanism requires involving competent domestic authorities in the adjudicating process and deferring to their opinion on the interpretation of relevant concepts.

Third, and finally, the proposed digital trade exception requires the EU's trading partners to recognise the protection of privacy and personal data as fundamental rights. Given that not all EU trading partners assign the same importance to these policy objectives, this provision is EU-centric. This thesis has proposed to rephrase this provision in a way that would allow the EU to maintain its high level of privacy and personal data

protection as fundamental rights while allowing other parties to adopt a lower level of protection if they so choose.

4. Some form of restrictions on transfers of personal data outside the EEA constitutes a part of the essence of the fundamental rights to privacy and the protection of personal data under the EU Charter. However, the actual design of the framework for such transfers is not a part of such essence. Although Article 52(1) of the EU Charter places some constraints on the EU legislator, the latter has sufficient flexibility to reform the GDPR rules governing transfers of personal data outside the EEA. This is necessary in order to make those rules more scalable and apt for performing their constitutional function of preventing the circumvention of 'effective and complete' protection of the fundamental rights to privacy and the protection of personal data in the EU. The thesis proposes three lines of thought for accomplishing this reform corresponding to a short, medium, and long term strategy.

Section 5.2 concludes that the EU Charter, as EU primary law, and the GDPR, as EU secondary law, are in a dynamic relationship with each other. While the GDPR has been adopted to effectuate the fundamental right to the protection of personal data (and other rights enabled by it), interpretation of its rules and the rules of the 1995 Data Protection Directive has informed the constitutional content of that fundamental right. To illustrate the point, from a mere constitutional interpretation of the secondary law concept of 'adequacy', the standard of 'essential equivalence' has become the constitutional benchmark and an instantiation of the strict necessity and proportionality requirements under Article 52(1) of the EU Charter in respect of the *whole* secondary law framework on transfers of personal data outside the EEA.

Next, Section 5.2 concludes that restrictions on transfers of personal data *per se* constitute a part of the essence of the fundamental rights to privacy and the protection of personal data, as their complete absence allows these rights to be easily circumvented and deprives them of their content. However, the *particular design* of those restrictions, as well as the standard of 'essential equivalence' setting constitutional boundaries on such a design, do not constitute a part of the essence of the above-mentioned fundamental rights. Based on the current CJEU case law, Section 5.2 argues that in order to respect the essence of the fundamental rights to privacy and the protection of personal data, the EU secondary law framework for transfers of personal data outside the EEA must incorporate the following elements:

• provide for some limitations on transfers of personal data outside the EEA and on onward transfers,

• contain safeguards preventing generalised access of foreign authorities to the content of electronic communications,

• ensure that purposes for processing personal data are limited,

• require that the processing of personal data is accompanied by rules designed to ensure, inter alia, the security, confidentiality and integrity of the data, and also to protect them against unlawful access and processing,

• not permit retention of the content of communications, and

• provide for some possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data.

Using the constitutional function of the EU rules for transfers of personal data to prevent the circumvention of the 'effective and complete' protection of privacy and personal data in the EU, Section 5.3 identifies several weaknesses of those rules. These weaknesses are put in the context of broader political, societal and technological changes between 1995 (when those rules were first adopted) and 2020. First, this thesis argues that the CJEU *Schrems II* judgement has reinstated – on the books – the logical consistency of the tools for systematic transfers of personal data: the adequacy mechanisms, and appropriate safeguards under Article 46 of the GDPR, such as the SCCs and the BCRs. However, in practice, this judgement would either lead to the increased localisation of personal data in the EEA or to a fairly low level of compliance - on the ground. The problem is that, as a matter of fact, data will continue flowing across borders. At the same time, (most) companies have insufficient expertise and resources to ensure that all personal data transferred on the basis of appropriate safeguards is safeguarded the level of protection abroad that is essentially equivalent to the protection in the EU. Furthermore, the DPAs have neither the financial nor the human resources to monitor such compliance. If individuals resort to private enforcement, including mass claims, to compensate for lack of public enforcement – which is increasingly the case – interpretation of the 'essential equivalence' standard in relation to transfers of personal data to various third countries by different EU member states courts is likely to lead to a fragmentation of the EU regime for transfers of personal data. Section 5.3, therefore, argues that the problem of foreign surveillance, which lies at the core of this issue, should rather be addressed by the EU and its trading partners in an international forum, which should not coincide with international trade negotiations.

Second, the thesis argues that the adequacy framework itself suffers from political pressures as well as from what the thesis has called the 'snapshot', the 'heavy burden', and the 'onward transfer' problems. Third, and more generally, the thesis contends that the EU framework for transfers of personal data outside the EEA lacks granularity in the sense that the same rules apply irrespective of the context, volume and type of data transferred, and other parameters of data transfers. In a world where massive volumes of various kinds of

personal data are transferred every second, it is unrealistic to expect that the stringent EU framework under Chapter V of the GDPR will be fully observed, and most importantly, monitored and enforced by authorities in all those transfers.

Section 5.4 suggests and elaborates upon three possible lines of thought on how to improve the current GDPR framework for transfers of personal data outside the EEA. The first, and the most moderate, line of thought proposes to improve *specific* elements of mechanisms for transfers of personal data, without changing the design and composition of the framework. In particular, it proposes:

1. to adopt a transparent procedure governing adequacy assessment to address proneness of adequacy mechanism to political influence;
2. to transition adequacy assessments from a unilateral instrument to a reciprocal agreement, under which the foreign country would undertake certain obligations, such as to notify about any changes in legislation considered during the adequacy assessments, and to accept negative consequences of the failure to notify;
3. to ensure that onward transfer mechanisms in adequacy decisions, as much as possible, mirror the appropriate safeguards provided for in the GDPR and as interpreted by the CJEU in *Schrems II*. Consent should not be allowed as a legal ground for systematic onward transfers;
4. to reform the SCCs to meet the GDPR standards and to issue practical guidance on additional measures that could be taken to compensate for absence of 'essentially equivalent' protection of personal data in third countries that have not been afforded an adequacy decision.

The second, intermediate, line of thought proposes to add greater scalability to the framework while improving its particularities. It requires a more substantial revision of the GDPR and, therefore, could realistically be addressed only in the medium term – for example, in the next review of the GDPR's Chapter V under Article 97 GDPR in 2024. In addition to the reform proposals outlined in the first line of thought, the second line of thought proposes two principle adjustments to Chapter V of the GDPR:

1. introducing more lenient rules for transfers of personal data in relation to pseudonymised data, with the exception of pseudonymised sensitive data, and data in transit; and
2. giving legal significance in Chapter V of the GDPR to technological means for protection of personal data, including as a means of ensuring that pseudonymised data will not be re-identified after the transfer.

The third, long term, line of thought proposes a more fundamental redesign of the EU framework for transfers of personal data. One way of doing so would be to replace the

current one-size-fits-all approach, in which different mechanisms for transfers of personal data do not take into account the context and the parameters of the transfer, with rules designed on a *risk-based approach*, which is already implemented in some GDPR provisions. In the light of the constitutional function of the EU framework for transfers of personal data, as mentioned above, the main risk that the redesigned framework should address is the circumvention of the 'effective and complete' protection of privacy and personal data protection that the EU affords, when personal data is transferred abroad. Reformulating this in fundamental rights term, it is a risk that transfers of personal data outside the EEA can interfere with the fundamental rights to privacy and the protection of personal data more than is strictly necessary and proportionate to pursue a legitimate public policy objective. Safeguards required for transfers of personal data could be differentiated depending on the remoteness of link between personal data and the individuals to which it relates or, in other words, on the risk of the reidentification of individuals and threat of harm to their fundamental rights.

Avenues for further research

This thesis has aimed to demonstrate the need to reform the EU framework for transfers of personal data outside the EEA in Chapter V of the GDPR, and situated it within the context of international trade law and the reform of trade law, including the EU's proposed model clauses for future trade agreements. In the case of the GDPR, an effort based on a host of both domestic and international factors that goes well beyond this work, is needed to design a fully-fledged reform proposal.

Beyond strictly legal questions, cross-border transfers of personal and other data also raise questions of social justice, especially in the context of using personal data to develop, fine-tune, and regulate the use of AI systems. So far, privacy and data protection are the only policy objectives that are juxtaposed with those of digital trade liberalisation in EU digital trade discourse. However, in designing exceptions from data flow provisions, questions of who benefits and who loses from data flows should also be considered, especially in a multilateral setting. Put simply, research is necessary to explore how distributional issues should be incorporated in the design of digital trade provisions.

Finally, national security interests are increasingly taking centerstage in governments' policy on data flows and trade policy. This topic has four dimensions. First, national security concerns lead some governments, like the United States, to restrict transfers of personal data to non-democratic countries like China, viewing such transfers as a national security threat. Second, the United States' national security programmes, which allow the US authorities to access Europeans' data for national security purposes, recently led the CJEU to invalidate the most commonly-used mechanism for transfers of personal data to the United States – the EU – US Privacy Shield (*Schrems II* judgment).

Similarly (albeit for different reasons), as mentioned in Section 5.4, DPAs across Europe are investigating TikTok's data processing practices in Europe, and specifically transfers of personal data to China. Third, as recently confirmed by the CJEU in the *Schrems II* and *Privacy International* cases, the EU Charter guarantees under Articles 7 and 8 apply to rules governing surveillance authorities' access to personal data for national security purposes, when such data is obtained by authorities from private parties (such as telecommunication services providers or platforms), both under EU member states law and the law of foreign states receiving personal data from the EEA. Fourth, the national security exception plays a special role in international trade agreements due to its breadth, and it is has been invoked recently by countries trying to derogate from their trade commitments for reasons only marginally related to national security. Furthermore, as discussed in Chapter 4, the US has broadened the national security exception in its digital trade agreements by removing the factual circumstances in which it can be invoked, present in the WTO exception, thus removing an important objective constraint on the invocation of the exception. At the same time, cross-border data flows are increasingly regulated by international trade agreements, which means that, in a trade setting, countries could potentially invoke a national security exception to restrict data flows as well. As a result, there is a tension between the tendency, on the one hand, to keep the national security exception as broad as possible due to the quintessential importance of national security for the very existence of the states and, on the other hand, to use the national security exception as a means to derogate from the increasingly broader scope of trade commitments on the grounds unrelated to traditional security interests. This tension will either lead to the narrowing of the regulatory autonomy of states to invoke national security, or erode the foundations of the rule-based multilateral trading system. Using the issue of cross-border data flows as a case study to demonstrate how national security concerns can drive countries towards imposing data localisation, further research is needed to consider whether a reform of the national security exception in trade agreements is necessary. This research could also include finding an international law solution to the problem of foreign surveillance authorities' access to personal data from companies that received such data in the course of conducting business.