Governing cross-border data flows

Reconciling EU data protection and international trade law

Iakovleva, S.

Publication date
2021

Short Summary

GOVERNING CROSS-BORDER DATA FLOWS:

RECONCILING EU DATA PROTECTION AND INTERNATIONAL TRADE LAW

This thesis explores the difficulty of reconciling two important legal and policy objectives of the European Union. On the one hand, the EU Charter of Fundamental Rights (EU Charter) guarantees the protection of the rights to privacy and the protection of personal data as fundamental rights. On the other hand, in its external trade policy the EU seeks to liberalise cross-border data flows and to maintain and further develop a globally binding rules-based trading system that ensures appropriate access to foreign markets for EU businesses. Until recently in EU external policy, the two objectives had little in common and, therefore, did not come into conflict. In recent years, however, as cross-border flows of personal and other data have become 'the lifeblood of international trade', those conflicts have now emerged. Indeed, the area of digital commerce is taking up a growing share of world trade. Yet the collection and commercial use of personal data also implicates essential noneconomic values. Those values explain why personal data is protected by the EU Charter, and why it was instantiated with a high degree of specificity by the General Data Protection Regulation (GDPR). The thesis examines how these two objectives may be pursued simultaneously.

Although individuals can gain from the free flow and ubiquitous monetisation of their data by companies – for example, in the form of personalised services – they also have a lot to lose. From a global perspective, massive cross-border appropriation of personal data has been compared to resource extraction. Potential damage to individuals, and to society as a whole, far transcends the direct economic losses suffered from data breaches and identity threats.

Since 2009, the right to the protection of personal data has been a binding fundamental right in the EU, that is, separate from the (also fundamental) right to privacy. Just as personal data has both economic and societal value, the European data protection regime has a dual objective: protecting the fundamental rights and freedoms of individuals (in particular their right to the protection of personal data), and ensuring the free flow of personal data within the European Economic Area (EEA). However, the constitutionalisation of the EU has brought the non-economic goals of current European data protection law to the fore, placing them ahead of economic needs. Recently, robust protection of the fundamental rights to privacy and personal data has formed part of the EU response to growing concerns about technological or digital sovereignty with regard to the growing economic and social influence of non-EU (primarily American) technology companies.

There is a countervailing view that domestic restrictions on international data flows in general, and on personal data flows in particular, are a form of undesirable 'protectionism'. That view is now front and centre in academic, public and policy conversations on the topic, as the focus of international trade negotiations shift to digital trade. The push for international trade law to liberalise international flows of personal and other data is seen as being at odds with legal regimes that restrict such flows on privacy and data protection grounds, especially that of the European Union. Unlike the internal trade liberalisation *within* the EU single market (which led to the emergence of the EU data protection framework in the past), the EU's external trade liberalisation goal is in tension with the EU data privacy law, due to their opposite normative valences.

The World Trade Organization (WTO) is the main body administering international trade rules. Both the EU and its member states are WTO members. However, the WTO's role has recently decreased due to political circumstances and the multiplication of regional and bilateral trade agreements. So-called 'new generation' free trade (such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement), entered into by the EU's most important trading partners, such as Canada, Japan and the US, include provisions obliging parties to allow free cross-border flows of information, including personal data. Cross-border data flows are also high on the agenda in the recently launched negotiations on e-commerce at the WTO.

The elimination of restrictions on data flows has been one of the most contentious issues in many recent trade negotiations in Asia, Europe, and North America. With the international trade regime increasingly moving towards 'free' digital trade, and the Court of Justice of the European Union (CJEU) asserting the protection of EU fundamental rights as a pre-requisite for such transfers, this thesis argues that the risk that the EU's commitment to liberalising the cross-border movement of services under the General Agreement on Trade in Services (GATS), on the one hand, and to the protection of the fundamental right to the protection of personal data, on the other hand, will clash is very real. This clash is not in and of itself a reason to cry foul. Both the EU Charter and international trade law contain exceptions that allow each system to tolerate encroachments on their respective rules by the other, within certain limits. The majority of international trade agreements, including the GATS, provide for a so-called 'general exception'. This exception preserves the regulatory autonomy of parties to an international trade agreement and enables them to adopt and maintain measures 'necessary' to protect the privacy of individuals in relation to the processing and dissemination of personal data, even if such measures run counter to the member's international commitments (the trade necessity test). Article 52(2) of the EU Charter, in turn, allows the EU to limit fundamental rights if this is 'necessary' to meet objectives of general interest to the EU or to protect the rights and

freedoms of others (the EU Charter necessity test). However, as this thesis argues in Chapter 2, the trade necessity test, as interpreted by the WTO adjudicating bodies, could be insufficient to safeguard the EU's autonomy to protect the fundamental right to data privacy under the EU Charter.

In 2018, in search of a better alternative, the EU developed horizontal provisions on cross-border data flows and the protection of privacy and personal data for its prospective digital trade agreements. The EU has tabled these model clauses in digital trade negotiations with its trading partners ever since (for example, with Australia, Indonesia, New Zealand, Tunisia and the UK), and included them in the EU proposal for the WTO rules on electronic commerce. The EU's proposed model clauses contain a narrower prohibition on restrictions of cross-border data flows than the US approach (which has been implemented in the CCTPP, the USMCA, and the US-Japan Digital Trade Agreement), and an exception for domestic privacy and data protection rules which is significantly broader than the above-mentioned general exception (also replicated in the US model).

Against this backdrop, the primary research question answered in this thesis is:

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?

The thesis answers the question by addressing the four sets of sub-questions, answered sequentially in Chapters 2-5.

Chapter 2 identifies and sets out the key issue underlying this thesis: namely that of the increasing tension between the governance of cross-border transfers of personal data by EU and international trade law. It develops the argument that EU restrictions on transfers of personal data could conflict with the EU's commitments under the GATS and post-GATS trade agreements. It contends that such restrictions are unlikely to meet the trade necessity test even in its most lenient interpretation because they arguably go beyond the limits set by the GATS provisions and the general exception for privacy and data protection. At the same time, under the strict necessity test contained in the EU Charter (as interpreted by the CJEU), the regulatory autonomy under EU law to derogate from the protection of the fundamental rights to privacy and the protection of personal data may be insufficient to comply with the EU's international trade obligations when it comes to cross-border flows of personal data. The sequential application of the two 'necessity tests' creates a risk that the two 'necessities' may clash, putting the EU in a catch-22 compliance deadlock between the violation of trade law or unjustifiable derogation from the fundamental right to the protection of personal data, as construed by the CJEU.

In the context of the ongoing digital trade negotiations that the EU is conducting with its trading partners on cross-border data flows, privacy and data protection, this state of affairs is not sustainable. Under EU primary law, EU institutions may not negotiate international trade rules inconsistent with the EU *acquis*. At the same time, despite international trade agreements ranking below EU primary law in the hierarchy of EU law, the EU cannot be relieved of its international trade obligations for the sole reason that they are inconsistent with EU primary law. Therefore, the EU should be able to comply with the Charter *and* its international trade obligations *simultaneously.* The path forward suggested in this thesis, and further elaborated on in Chapters 3 and 4, is guided by three principal considerations. First, from a practical perspective, it is risky to wait until EU restrictions are struck down by – or even challenged by – an international trade adjudicating body, which would force the EU's hand and possibly impose an unrealistic reaction timeframe. A more proactive approach seems preferable. Second, and relatedly, ongoing uncertainty surrounding the lawfulness of transfers of personal data outside the EEA, on the one hand, and compliance with the restrictions on such transfers with the EU's international trade commitments, on the other hand, may have a chilling effect on cross-border trade to the detriment of EU businesses. Third, although the approach to transfers of personal data outside the EEA that would make the most solid contribution to the 'effective and complete' protection of the fundamental rights to privacy and the protection of personal data is a total ban on such transfers, this rather extreme approach would undermine the very existence of digital cross-border trade with the EU and is thus unwarranted.

Chapter 3 takes a step back and investigates what the term 'protectionism' entails and whether EU restrictions on transfers of personal data outside the EEA are protectionist. Applying insights from the work of Michel Foucault on the relationship between discourse and power, this Chapter demonstrates that it is not possible to strike the right balance between digital trade liberalisation and the protection of data privacy by simply ruling out 'protectionism'. Chapter 3 also argues that the distinction between protection and protectionism is not clear-cut: the placing of the line between protection and protectionism is ultimately a judgement call. On a spectrum between the two extremes, there is a grey area that includes domestic measures, with an element of uncertainty as to what type of regulatory goal is at stake: protectionism in disguise or genuine protection, which only incidentally benefits domestic industries. Whether measures in this grey area should fall under the label of 'protection' or 'protectionism' – in other words, whether trade adjudicating bodies should err on the side of protection or protectionism – essentially depends on the discourse. Within an economic discourse, where free trade alone is high on the value scale, such regulation would be excluded as protectionist. In contrast, in a pluralist discourse where equal value is assigned to free trade and protection of

fundamental rights, allowing some mildly protectionist measures to go unchallenged in order to safeguard states' domestic autonomy to adopt socially beneficial regulation may be a preferred approach.

Therefore, the choice of the right discourse for policy conversations on domestic privacy and the protection of personal data, in the context of negotiating and interpreting international trade law, is crucial. The value structures attending it will ultimately strongly affect 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. Against this backdrop, Chapter 3 asserts that countries should be conscious of the value frameworks that come with a certain discourse and should ensure that their mutual values determine such discourse, as opposed to the other way around. This Chapter contends that the distinction between privacy and personal data protection, and protectionism is in part a *moral* question, that is, not just a question of economic efficiency. Therefore, when a policy conversation, such as the one on cross-border flows of personal data, involves non-economic values such as individual rights, the conversation should *not* be confined within the narrow field of trade economics but rather placed in a broader normative perspective.

On the subject of restrictions on cross-border flows of personal data, Chapter 3 argues that such restrictions are, and will remain, necessary. Unless approaches to data protection and privacy are harmonised, countries need more regulatory space to determine the design of domestic data protection regimes. It is precisely because data protection standards in other countries are low (perhaps strategically low) that countries with higher standards need to impose restrictions on personal data transfers.

Chapter 4 turns to the specific international trade law aspects of the problem identified in Chapter 2. It is divided into three parts. In the first part, this Chapter questions whether the model clauses on cross-border data flows and the protection of privacy and personal data, proposed by the European Commission in 2018, would allow the EU to overcome the potential catch-22 compliance deadlock in future trade agreements, while at the same time pursuing the goals of facilitating cross-border data flows and promoting a rules-based multilateral trading system. It argues that, superficially, the 2018 clauses do seem to provide the EU with the broad autonomy to protect privacy and personal data as fundamental rights while outlawing a number of measures restricting cross-border data flows. Compared to the US model, the prohibition of restrictions on cross-border data flows in the EU proposed clauses is formulated more narrowly. Furthermore, the proposed clauses assert that the normative rationale for the protection of personal data and privacy is the protection of fundamental rights. In addition, the breadth of the proposed exception for privacy and data protection (referred to as the 'digital trade exception'), modelled after

the national security exceptions in the WTO Agreements, secures the EU's ability to maintain restrictions on transfers of personal data outside the EEA under the GDPR. The proposed digital trade exception explicitly recognises the rules for cross-border transfers of personal data as an example of the types of measures that would be allowed under the exception.

The first part of Chapter 4 contends, however, that the proposed model clauses suffer from at least three essential flaws that could make them unable to safeguard the fundamental rights to privacy and the protection of personal data, and that undermine the goals of the EU digital trade policy, as identified above. First, the imprecise nature of the relationship between the proposed digital trade exception for privacy and data protection (intended for the digital chapters of trade agreements) and the general exception (typically included in the exceptions chapter of the same proposed trade agreements), creates legal uncertainty as to the material scope of the proposed exception. Second, the breadth of the proposed digital trade exception for privacy and data protection may nullify the impact of the proposed provision on cross-border data flows in the same model clauses. More generally, Chapter 4 argues that using the extremely low threshold of national security exceptions as a model for a digital trade exception for privacy and data protection could further undermine the stability of the rules-based international trading order. Third, the proposed model clauses are overly EU-centric in the sense that they require a recognition of the protection of privacy and personal data as fundamental rights – a commitment that not all EU trading partners may be willing to accept or implement in practice.

In the second part, Chapter 4 suggests three ways to improve the proposed model clauses. First, future trade agreements should either include a provision clarifying the relationship between the general and the digital trade exceptions for privacy and data protection, or contain a single exception for privacy and data protection which would apply throughout the agreement (acknowledging that the latter could be problematic in practice). Second, in the course of negotiations, the EU should consider replacing the 'it deems appropriate' threshold of the digital trade exception for privacy and data protection with a threshold which is higher than the 'it deems appropriate' standard but lower than the necessity test standard of the general exception. Third, the provision requiring the parties to recognise that the protection of personal data and privacy is a fundamental right should be rephrased in a way which, on the one hand, safeguards the EU's autonomy to maintain its fundamental rights protection of these rights but, on the other hand, allows other trading partners to adopt a lower level of protection (within international human rights law bounds) if they so choose.

In the third and final part, Chapter 4 considers thresholds other than the 'it deems appropriate' test, that the EU could fall back on without compromising on the fundamental

rights to privacy and data protection. It looks at other alternatives found in WTO agreements and bi-lateral and regional trade agreements, that are on the continuum between the 'necessity' in the general exception (the current test for privacy and data protection), and the 'it deems appropriate' test proposed for a digital trade exception for privacy and data protection by the EU. Chapter 4 argues that the standards of non-circumvention, non-avoidance and reasonableness could be viable alternatives to the 'it deems appropriate' standard, provided that they are accompanied by appropriate restrictive mechanisms constraining the discretion of trade adjudicators, and are applied in a nuanced manner.

Building on the conclusions of previous chapters, **Chapter 5** addresses the problem of the 'two necessities' identified in Chapter 2 of the thesis, from both an EU Charter and EU data protection law perspectives. The analysis in this Chapter is structured along the following three broad issues: (1) the constitutional boundaries the EU Charter imposes on EU secondary data protection law and specifically the extent to which the EU framework for transfers of personal data outside the EEA in the GDPR can be changed within such boundaries; (2) the ability of this framework to perform its constitutional function to prevent circumvention of the high level of personal data protection in the EU and, ultimately, to ensure 'effective and complete' protection of fundamental rights; and (3) the reform proposal for such a framework in response to changed political, geopolitical and economic circumstances.

On the first issue, Chapter 5 argues that there is a dynamic relationship between the GDPR (as a secondary EU law instrument) and the EU Charter (as a primary law instrument). At the same time, this Chapter demonstrates that the framework for transfers of personal data outside the EEA in Chapter V of the GDPR represents only *one* possible design of such a framework in the light of the EU Charter requirements. Only the presence of *some* restrictions, and a few aspects of such restrictions, constitute the essence of the fundamental rights to privacy, the protection of personal data and the right to judicial remedy (in the context of the first two rights), and therefore cannot be altered by EU secondary law. Other elements of such a framework can be determined by the EU secondary legislator on the basis of strict necessity and proportionality assessment, with the aim of ensuring its constitutional function, which is to prevent circumvention of the high level of personal data protection in the EU. The concept of 'essential equivalence', which, following the CJEU's *Schrems II* judgement, can be seen as the constitutional benchmark for the secondary law framework on transfers of personal data, does not constitute a part of the essence of the above-mentioned fundamental rights. Instead, it governs the balancing of the above-mentioned fundamental rights against competing policy objectives: primarily the economic benefits inherent in unrestricted cross-border flows of personal data, and the national security interests of foreign countries. Chapter 5, therefore, contends that the EU legislator has sufficient wiggle room to change the design

of the rules currently codified in Chapter V of the GDPR.

In the second part, Chapter 5 identifies four weaknesses in the EU framework for transfers of personal data outside the EEA. The first weakness is that, despite the recent *Schrems II* decision, there is a persistent qualitative gap between the adequacy decisions on the one hand, and the appropriate safeguards under Article 46 of the GDPR on the other (both of which serve as mechanisms for systematic transfers). The EU should address the foreign surveillance problem – which is the main reason why issues relating to transfers of personal data land at the CJEU – on the international level rather than through its own secondary law. The second weakness is that adequacy decisions are prone to political pressures in the context of EU trade policy. The third weakness is that adequacy decisions are unable to perform their constitutional function due to lack of regular reviews of the assessment on which the adequacy decisions are based (the 'snapshot' problem), the difficulties of enforcing individual rights in foreign jurisdictions (the 'heavy burden' problem), and the inadequacy of onward transfer mechanism embedded in the adequacy decisions (the 'onward transfer' problem). The fourth and last weakness is, on a more abstract level, the limited scalability of the current regime for personal data transfers in Chapter V of the GDPR in view of the technological developments that have occurred since the 1990s, when the core of the framework was first designed.

In its third and final part, Chapter 5 proposes three directions of thought on how to improve the framework of Chapter V of the GDPR within the boundaries set by the EU Charter, reflecting possible short, medium, and long term strategies for the EU in this area.

The first, and 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. For example, it proposes the adoption of a transparent procedure governing adequacy assessment to address the proneness of the adequacy mechanism to political influence and to transition adequacy assessments from a unilateral instrument to a reciprocal agreement. The second, intermediate, line of thought proposes adding 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: more lenient rules for transfers of non-sensitive pseudonymised data and giving legal significance to technological means for protection of personal data. 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.

Chapter 6 offers conclusions structured as responses to the main research question and sub-questions. The thesis concludes 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. The thesis paves the way for further research necessary in order to design a fully-fledged reform proposal of the EU framework for transfer of personal data outside the EEA. Chapter 6 also suggests an examination of the issues of social justice in the context of commercial use of personal data and of the increasingly intertwined relationship between national security, state surveillance, data privacy and international trade.