



## UvA-DARE (Digital Academic Repository)

### Governing cross-border data flows

*Reconciling EU data protection and international trade law*

Yakovleva, S.

### Publication date

2021

[Link to publication](#)

### Citation for published version (APA):

Yakovleva, S. (2021). *Governing cross-border data flows: Reconciling EU data protection and international trade law*.

### General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

### Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

## 1. Introduction

Between 2014-2016, a wave of protests swept across Europe. In Brussels, Amsterdam, Rome, Barcelona, Berlin, and more, thousands of people filled the streets chanting slogans: ‘Stop TTIP, TiSA & CETA now!’ ‘No TTIP, TiSA & CETA!’ ‘We need TTIP like a fish needs a fishing rod!’ The source of the public discontent was the ‘new generation’ of trade agreements that the EU was covertly negotiating with some of its most important trading partners: the Transatlantic Trade and Investment Partnership (TTIP) with the United States, the Comprehensive Economic Trade Agreement (CETA) with Canada, and the Trade in Services Agreement (TiSA) with 22 members of the World Trade Organisation (WTO), together representing approximately 70 per cent of world trade in services.<sup>1</sup> The protests were sparked not only by the substance of the agreements, namely their perceived threats to EU domestic policy in areas such as the environment, agriculture, culture and the media, but also by the process that created them, namely its secrecy and lack of democratic legitimacy and accountability. Although the possible implications of these agreements – primarily TTIP and TiSA – on the EU *acquis* and policy on privacy and data protection escaped the eye of the broader public at that time, they did not go unnoticed by either digital rights and consumer organisations and activists, or by EU institutions not involved in those trade negotiations.<sup>2</sup> For the first time, the tension between the liberalisation of digital trade, on the one hand, and data privacy, on the other, became a broader political issue rather than just a topic of a theoretical debate.

This thesis explores the difficulties in reconciling these 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<sup>3</sup> as fundamental rights. On the other hand, in its external trade policy, the EU seeks liberalisation of cross-border data flows, maintaining and developing a globally binding rules-based trading system to ensure appropriate access to foreign markets for EU businesses. The fundamental rights protection of data privacy in the EU originated as a prerequisite for the free flow of personal data in the internal market. It was, in other words, intertwined with the economic goals underlying the union. In EU external policy however, until recently, the two objectives had little in common and, therefore, did not come into

---

<sup>1</sup> EUROPEAN COMMISSION, Trade in Services Agreement (TiSA), <https://ec.europa.eu/trade/policy/in-focus/tisa/>

<sup>2</sup> See e.g. EDRI (2015); EDRI (2016); Ling (2016); European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)); European Parliament resolution of 3 February 2016 containing the European Parliament’s recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

<sup>3</sup> Throughout this thesis, the fundamental rights to privacy and the protection of personal data will also be jointly referred to as fundamental rights to data privacy.

conflict. The change was caused by the fact that cross-border flows of personal and other data have become the ‘lifblood of international trade’.<sup>4</sup> The area of digital commerce is taking up a growing share of world trade.<sup>5</sup> 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). Specifically, the thesis examines how these two objectives might be pursued simultaneously.

This topic is highly relevant to current policy debate in the EU on the data privacy implications of cross-border data flows, which takes place against the backdrop of ongoing digital trade negotiations with several trading partners, and the trade policy review (of which digital trade is part) launched by the European Commission in June 2020.<sup>6</sup> Furthermore, digital trade is an important part of the EU industrial policy in the next four years.<sup>7</sup>

This thesis contributes to academic literature by undertaking a comprehensive analysis of the issue of cross-border data flows from an EU data protection and international trade perspective, thus bridging the compartmentalisation of these two areas of law. As compared to existing literature, which typically takes either an international trade or a data protection perspective, this thesis undertakes an in-depth engagement with both areas of law with a specific emphasis on the interaction between them. This approach allows the thesis to propose ways of bridging the gap between international trade and EU rules governing cross-border data flows while preserving the normative values underlying each of these sets of rules.

The societal relevance of this work lies in the necessary reconciliation of European citizens’ rights, guaranteed under the EU Charter, with the realities of global digital commerce which will contribute to economic growth and job creation. The governance of cross-border flows of personal data must be at once solidly anchored in EU law and values, and capable of being ported to the trade law field. This is important because the outcome of trade negotiations will affect each and every person in the EU, as almost everybody uses the internet. Guaranteeing sufficient protection of fundamental rights whilst ensuring that society can benefit from digital commerce is the difficult challenge that this thesis aims to meet.

---

<sup>4</sup> Casalini, López González (2019), pp. 8,14.

<sup>5</sup> Manyika, Lund, Bughin, Woetze, Stamenov, Dhingra (2016), pp. 30-32.

<sup>6</sup> European Commission, *A renewed trade policy for a stronger Europe*. Consultation Note, 16 June 2020, pp. 7-8.

<sup>7</sup> Communication from the Commission, *A New Industrial Strategy for Europe*, COM/2020/102 final, 10 March 2020.

## 1.1 Setting the scene: background and problem definition

### 1.1.1 *International trade in data: what's at stake?*

The commercial use of personal data enables digital trade and contributes to economic growth. It may also generate individual benefits. However, those benefits often seem both remote and indirect when compared to the risks posed to individuals by the misuse of their data, such as identity theft, access to data by foreign surveillance and law enforcement authorities, profiling, unwanted marketing communications, discrimination, and denial of access to essential services, to name just a few. Unlike data, which can simultaneously be present in multiple locations and fall under the jurisdiction of multiple legal regimes, individuals retain a close connection with a particular State through the institutions of citizenship or residency. It is first and foremost *that* State that must guarantee the individuals' human rights and protect them from the undue actions of other States. The level of fundamental rights protection that individuals can expect in the EU member states may not necessarily be upheld once personal data is processed in other countries, such as the US, China or Russia. Simply put, while trade in data is *international*, protection of individual rights largely remains the prerogative of *domestic law*,<sup>8</sup> especially when it comes to the protection of the fundamental rights to privacy and the protection of personal data. Although these rights are recognised by important international<sup>9</sup> and regional<sup>10</sup> human rights law instruments, and governed by several regional guidelines,<sup>11</sup> countries across the globe still have important disagreements on the normative rationales underlying the protection of the two rights and the approaches to transfers of personal data.

Cross-border trade in digital goods and services is increasingly dependent on personal data. Globalisation and the decentralisation of production and distribution value chains have made the cross-border movement of information – commercial, machine-generated and personal – crucial for the production and provision of services, both online and offline,<sup>12</sup> as well as the day-to-day management of companies. Projecting this economic reality, promising unprecedented efficiency gains, economic development and growth, onto a global legal landscape compartmentalised by multiple domestic legal systems, is a sobering exercise. When set against the economic benefits driving globalisation, these legal systems must consider how these benefits fit into a broader set of national and regional priorities, such as national security, fundamental rights protection, industrial policy, and cultural values. Differences in the relative weight accorded to each

---

<sup>8</sup> In this thesis, the EU *acquis* is also referred to as 'domestic' law.

<sup>9</sup> Art. 12 UDHR; Art. 17 ICCPR.

<sup>10</sup> Art. 8 ECHR; Convention 108+.

<sup>11</sup> The OECD Privacy Framework (2013); APEC Privacy Framework (2015); APEC Cross-Border Privacy Rules System (CBPR) (2019).

<sup>12</sup> Helberger, Zuiderveen Borgesius, Reyna (2017), pp. 1430-1431.

of those priorities vis-à-vis the economic and political gains from cross-border data flows have resulted in a diverse set of diverging domestic rules governing such flows, especially when it relates to identified or identifiable individuals (that is, the definition of personal data in the GDPR).

Companies doing business globally face the challenges of compliance with several data protection regimes and rules for cross-border transfers of personal data in several countries. Having a lot to gain from dismantling restrictions on the free flow of data, a plethora of industry-funded think-tanks try to shape the global policy agenda by painting a grim picture in which protection of data privacy is framed as a barrier to trade and a threat to economic progress.<sup>13</sup> Using an often one-sided narrative of ‘digital protectionism’, surveillance capitalists portray their practices as ‘inevitable expressions of the technology they employ’<sup>14</sup> and digital globalisation as the next logical step of economic integration and development.<sup>15</sup> Individuals, on the other hand, must deal with the limitations of domestic legal systems to enforce their rights effectively against the misuse of their personal data on a global scale. Although individuals do also 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. The potential damage to individuals and society as a whole, transcends the direct economic losses from data breaches and identity threats. It includes discrimination and social exclusion; the undermining of human dignity by transforming human experiences into behavioural data; and the shaping of individuals’ behaviour and choices, both on the micro level of what news to read and items to buy, and on the macro level of expressing political *preferences*. From a global perspective, massive cross-border appropriation of personal data can be compared to resource extraction.<sup>16</sup> For example, Couldry and Mejias argue that cross-border data flows ‘are as expansive as historic colonialism’s appropriation of land, resources, and bodies, although the epicenter has somewhat shifted’.<sup>17</sup> In their view, the transformation of human actors and social relations formalised as data, into value, leads to power imbalance (between colonial power and colonised subjects).<sup>18</sup> Against this backdrop, as Morozov puts it, the EU’s ‘much-cherished commitment to data protection ... aimed, above all, at protecting citizens from excessive corporate and state intrusion – is increasingly at odds with the “grab everything” mentality of contemporary capitalism’.<sup>19</sup>

---

<sup>13</sup> See Morozov (2015).

<sup>14</sup> Zuboff (2019), p. 15.

<sup>15</sup> For a discussion, see Section 3.3.

<sup>16</sup> Couldry, Mejias (2019), pp. 337-338.

<sup>17</sup> *Ibid.* But see Mueller, Grindal (2019), p. 82, challenging this point of view.

<sup>18</sup> Couldry, Mejias (2019), pp. 337-338.

<sup>19</sup> Morozov (2015).

### 1.1.2 EU data privacy framework

Since 2009 (when the EU Charter took effect), the right to the protection of personal data has been a binding fundamental right in the EU (Article 8 of the EU Charter), separate from the fundamental right to privacy (Article 7 of the EU Charter).<sup>20</sup> The EU Charter has the highest legal status in the EU, on a par with the Founding Treaties. Just as personal data has both economic and societal value, the European data protection regime, first introduced by the 1995 Data Protection Directive, 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).<sup>21</sup> Conflicting at first glance,<sup>22</sup> these objectives are easier to reconcile if seen as cause and effect, or as the ‘why’ and the ‘how’. The harmonisation of data protection rules was a prerequisite for the free flow of personal data without undermining individuals’ rights to the protection of such data originating from EU member states affording a higher level of protection (the ‘why’).<sup>23</sup> The fundamental rights approach (‘the how’) sets the level of protection of personal data which the EU-wide personal data protection framework should attain. However, the constitutionalisation of the EU has put the economic needs that necessitated the creation of the EU-wide data protection framework in the first place, to the background, and emphasised the non-economic goals of the current European data protection law.<sup>24</sup> That said, the GDPR, adopted under the EU’s competence to legislate on the fundamental right to the protection of personal data, is still cited as one of the pillars of the EU Digital Single Market.<sup>25</sup> Recently, robust protection of the fundamental rights to privacy and personal data has also become a part of the EU response to a growing concern about ‘technological’ or ‘digital sovereignty’, with regard to the growing economic and social influence of non-EU (and primarily American) technology companies.<sup>26</sup> The EU is increasingly using technological or digital sovereignty labels ‘as a means of promoting the

---

<sup>20</sup> Despite the separation of the rights to privacy and the protection of personal data in the EU Charter, this thesis often refers to these two rights jointly. The issue on the relationship between these two rights has generated much academic debate but remains unresolved. For a recent recount of the state of this debate, see Lynskey (2020), pp. 29-32. For a deeper analysis of the intricate relationship between the two rights, see Lynskey (2015) pp. 89-106. For a comprehensive historical account of the issue, see González Fuster (2014).

<sup>21</sup> Art. 1 GDPR; Art. 1 Data Protection Directive. The European Economic Area consists of the Member States of the European Union and countries of the European Free Trade Association (EFTA) - Norway, Iceland and Lichtenstein. EUROSTAT, Glossary: European Economic Area (EEA), [https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European\\_Economic\\_Area\\_\(EEA\)#:~:text=The%20European%20Economic%20Area%2C%20abbreviated,force%20on%201%20January%201994](https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA)#:~:text=The%20European%20Economic%20Area%2C%20abbreviated,force%20on%201%20January%201994)

<sup>22</sup> See e.g. Macenaite (2017), pp. 506-507.

<sup>23</sup> Costa-Cabral, (2017), p. 17.

<sup>24</sup> Lynskey (2013). For further discussion, see Sections 2.2.1.1 and 2.3.3.

<sup>25</sup> Communication from the Commission, *Completing a Trusted Digital Single Market for All*, COM (2018) 320 final, 15 May 2018, pp. 2–3.

<sup>26</sup> Madiega (2020), p. 1. For a discussion on how this reflects in the EU trade policy, see Chapter 4.

notion of European leadership and strategic autonomy in the digital field'.<sup>27</sup> In the international arena, the EU's digital strategy, anchored in European values and fundamental rights, ties into the 'ideal of a social European model'<sup>28</sup> alternative to the American model of 'surveillance capitalism'.<sup>29</sup>

### *1.1.3 Tension between external trade policy and domestic data privacy framework*

The view that domestic restrictions on international data flows in general, and on personal data flows in particular, are a form of undesirable 'protectionism' 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'.<sup>30</sup> From this angle, unrestricted cross-border data flows promise global economic growth, and are often perceived as a *bonum in se*.<sup>31</sup> However, the tendency of international trade law to liberalise international data flows is at odds with legal regimes that restrict such flows on privacy and data protection grounds, especially that of the European Union.<sup>32</sup> As a result, the data flow issue has become 'the new battlefield'<sup>33</sup> between domestic legal regimes, not only between the United States and the European Union, but also between the European Union and its other trading partners.<sup>34</sup> While the debate often runs along the line of eliminating 'digital protectionism', there is an ideological divide on whether, and to what extent, data privacy protection should fall under or be excluded from the scope of this notion.<sup>35</sup>

Conflicts are thus bound to arise from the fact that, while international trade law

---

<sup>27</sup> *Ibid.* See also Communication from the Commission, *A New Industrial Strategy for Europe*, COM/2020/102 final, 10 March 2020, pp. 1,4; Communication from the Commission, *A European strategy for data*, COM(2020) 66 final, 19 February 2020; European Commission, *White Paper on Artificial Intelligence. A European Approach to Excellence and Trust*, COM(2020) 65 final, 19 February 2020, p. 3.

<sup>28</sup> Petkova (2019), p. 153.

<sup>29</sup> Zuboff (2019); Zuboff (2015); Madiaga (2020), p. 3.

<sup>30</sup> For further discussion see Section 3.3.

<sup>31</sup> *Ibid.*

<sup>32</sup> See, e.g., Swire, Litan (1998), pp. 188-193; Weber, Staiger (2017), pp. 58-59; Bergkamp (2002), pp. 39-40; Reidenberg (2001), pp. 735-738; Yakovleva, Irion (2016), pp. 202-207; But see Shaffer (2000), pp. 46-51 (arguing that a hypothetical US claim regarding WTO inconsistency of the EU's framework for personal data transfers 'would likely not prevail'); Perez Asinari (2002), p. 277; Chen (2015), pp. 218-219 (admitting that, although the EU regime for transfers of personal data may violate the EU's WTO commitments, such violation can be justified under the general exception).

<sup>33</sup> Burri (2017c), p. 408.

<sup>34</sup> For example, provisions on cross-border flows of information, including personal data, have been a contentious point in the negotiations of the JEFTA. See Bartl, Irion (2017). Not being able to reach an agreement in trade negotiations, instead of such provisions, the parties included a three-years review clause in the final version of the agreement. Aaronson, Leblond (2018), p. 261. Cross-border flows of personal data from the EU to Japan were ultimately regulated through an Adequacy Decision. For its data protection to be recognised as 'adequate' under EU law, Japan has amended its legislation and has undertaken additional commitments in the adequacy decision. The Adequacy Decision for Japan was adopted on 23 January 2019, shortly before JEFTA took effect. European Commission, Press Release: *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows*, IP/19/421, 23 January 2019.

<sup>35</sup> For a discussion see Section 3.3.

increasingly aims to liberalise data flows to facilitate digital cross-border trade, EU data protection law restricts cross-border transfers of personal data outside the EEA. Grounded in the fundamental rights to the protection of privacy and personal data under the EU Charter,<sup>36</sup> the rules for transfers of personal data outside the EEA aim to ensure that the level of protection guaranteed in the EU by the GDPR is not undermined as personal data leaves the EEA.<sup>37</sup> Although the GDPR does not explicitly refer to any fundamental right except for the fundamental right to the protection of personal data, this does not mean that the GDPR furthers this right alone. This is clear from recital 4 of the GDPR, which requires that the ‘processing of personal data should be designed to serve mankind’. Furthermore, the right to the protection of personal data itself enables a multitude of other fundamental rights and values.<sup>38</sup> This right is triggered by any processing of personal data (itself defined very broadly<sup>39</sup>), which is now integral to almost any societal activity. It is a proxy to a wide array of public policy interests from the protection of democracy, human dignity and personality rights, to obtaining a fair share of the economic value derived from personal data.<sup>40</sup> According to Rodotà, ‘[d]ata protection can be seen to sum up a bundle of rights that make up citizenship in the new millennium’.<sup>41</sup>

As a result, 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. EU data privacy law can tolerate transfers of personal data outside the EEA only to the extent that these transfers are compliant with the EU Charter and the GDPR. In turn, international trade law can tolerate the EU’s restrictions on personal data transfers only to the extent that they comply with the EU’s international trade liberalisation commitments, including possible exceptions thereto.

---

<sup>36</sup> CJEU, *Schrems I*, paras. 72-73; CJEU, *Schrems II*, para. 94; CJEU, *Opinion on EU-Canada PNR Agreement*, para 214.

<sup>37</sup> Art. 44 GDPR, CJEU, *Schrems I*, paras 72-73; CJEU, *Schrems II*, paras. 92, 94 See also González Fuster (2016), p. 168.

<sup>38</sup> Oostveen, Irion (2017); Ausloos (2018), pp. 62-63; Clifford, Ausloos (2018), p. 147.

<sup>39</sup> For a discussion see Section 5.3.3.

<sup>40</sup> See e.g. Lynskey (2014), p. 573-574; Rouvroy, Pouillet (2009), pp. 53-54, 57 (contending that the rights to privacy and data protection have ‘an “intermediate” rather than a “final” value, because they are “tools” through which more fundamental values, or more “basic” rights—namely human dignity and individual personality rights—are pursued;’ that the rights to privacy and personal data protection protect the fundamental value of personal autonomy against the threats of technological evolution, and that they constitute social structural tools for preserving a free and democratic society). See also Delacroix, Lawrence (2019); Hall, Pesenti (2017); Hardinges (2018); *Initiatiefnota van het lid Verhoeven over mededinging in de digitale economie*; *Motie van het lid Buitenweg c.s. over vormgeving van data trusts in Nederland*, 16 december 2019, KST351347, 35134, nr. 7 exploring data trusts as a means of sharing value obtained through commercial use of personal data.

<sup>41</sup> Rodotà (2009), pp. 77-80.

#### 1.1.4 Restrictions on personal data flows: a barrier to digital trade?

The WTO is the main body administering international trade rules.<sup>42</sup> Both the EU and its member states are parties to the Marrakesh Agreement establishing the WTO.<sup>43</sup> The WTO notably includes a binding dispute-settlement system. The current framework dates back to 1995 and does not regulate specifically cross-border data flows. However, general principles of trade law, such as most-favoured nation and national treatment or market access commitments under the General Agreement on Trade in Services (GATS), do apply to EU restrictions on cross-border data flows. However, the WTO's role has recently decreased due to political circumstances and the multiplication of regional and bilateral trade agreements. In response to rapid technological change, new international law obligations are emerging through bi- and plurilateral trade venues that by-pass the WTO. So-called 'new generation' free trade agreements, 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. These disciplines have, for example, been included in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),<sup>44</sup> and in the recent US-Mexico-Canada Agreement (USMCA),<sup>45</sup> and the US-Japan Digital Trade Agreement.<sup>46</sup> In all such agreements, a free data flow obligation is counterbalanced by an exception, strongly resembling that of the GATS Article XIV(c), that allows parties to derogate from it, in order to adopt and maintain regulation in the public interest.<sup>47</sup> There is also a movement afoot to update WTO rules. Cross-border data flows are high on the agenda in the recently launched negotiations on e-commerce in the WTO between 76 WTO members.<sup>48</sup>

Taking the view that domestic restrictions on cross-border flows of personal data are a barrier to reaping the benefits of global digital trade,<sup>49</sup> an increasing volume of literature either highlights the risk of inconsistency of personal data protection with the rules of the WTO, asks for new rules to ensure free flows of personal data across borders, or both.<sup>50</sup>

---

<sup>42</sup> WTO Agreement.

<sup>43</sup> Although the Marrakesh Agreement is a mixed agreement from an EU law perspective, Eckes explains that "this mixed nature has, in practice, been replaced by EU dominance". Eckes (2019), p. 186.

<sup>44</sup> Art. 14.11 CPTPP, which states: 'Each 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'.

<sup>45</sup> Under Art. 19.11 of the USMCA, '[n]o Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person'.

<sup>46</sup> Art. 11 of the US – Japan Digital Trade Agreement.

<sup>47</sup> Art. 14.11(3) CPTPP, Art. 19.11 USMCA, Art. 11(2) of the US – Japan Digital Trade Agreement.

<sup>48</sup> European Commission, 76 WTO Partners Launch Talks on E-Commerce, 25 January 2019.

<sup>49</sup> For a discussion on how data protection is being framed as digital trade barrier in the economic digital trade discourse, see Section 3.3.

<sup>50</sup> See Section 2.2.2.

The elimination of such restrictions remains one of the contentious issues of most recent trade negotiations in North America, Europe and Asia.<sup>51</sup> Meanwhile, as personal data has become an integral part of digital services, the EU constitutional protection of the rights to privacy and the protection of personal data (of which restrictions on personal data transfers is an important pillar), is actually strengthening.<sup>52</sup> As a result, with the international trade regime increasingly moving towards ‘free’ digital trade,<sup>53</sup> the risk that the EU’s international trade law commitments to liberalise the cross-border movement of services, on the one hand, and the protection of the fundamental rights to data privacy, on the other hand, will clash is very real.

The recent *Schrems II* judgement of the Court of Justice of the European Union (CJEU) invalidated, second time around, the EU-US legal framework for transatlantic flows of personal data, the EU-US Privacy Shield. It asserted a high legal standard for systematic transfers of personal data in general and created additional pressure on the EU approach to the governance of personal data transfers from an international trade law perspective. In reaction, one of the US commentators suggests that instead of engaging in further negotiations with the EU on its fundamental rights terms, the US should respond along the lines of international trade law and economic sanctions.<sup>54</sup> For example, the US should treat the CJEU’s judgement as a violation of the WTO rules and retaliate using available US trade law mechanisms or impose sanctions against the EU together with countries like UK, Canada, Australia and India.<sup>55</sup>

#### *1.1.5 Clash between EU Charter and EU international trade commitments*

A clash between the EU’s constitutional protection for personal data (as translated into a framework for cross-border transfers of personal data in the GDPR) and the EU’s trade liberalisation commitments 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. As long as the exceptions in both systems are aligned, they can limit the degree of tension between the two systems.

Most prominently among existing exceptions, the majority of international trade agreements governing trade in services provide for so-called ‘general exceptions’, which

---

<sup>51</sup> See e.g. Cerulus, Scott (2019); Pant, Sarma (2019); Fefer (2019).

<sup>52</sup> See Section 2.2.1.1.

<sup>53</sup> Some countries, such as India, the African group and the Least Developed Countries, however, are critical about the e-commerce provisions in trade agreements, including those liberalising cross-border data flows. See e.g. Work Programme on Electronic Commerce, Report of Panel Discussion on ‘Digital Industrial Policy and Development’: Communication from the African Group, JOB/GC/133, 21 July 2017; Saez, C. (2017).

<sup>54</sup> Baker (2020).

<sup>55</sup> *Ibid.*

are modelled after or incorporate *mutatis mutandis* the one contained in Article XIV of the GATS.<sup>56</sup> 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). In other words, trade rules start from the premise that cross-border flows should be free, and contain an exception that might allow the EU to protect personal data. 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). As interpreted by the CJEU, this provision allows EU bodies to conclude an international agreement, which involves transfers of personal data outside the EEA, if the conditions laid out in this clause and most importantly that the Charter’s necessity test, are fulfilled.<sup>57</sup> The EU Charter protects the fundamental right implicated by the processing of personal data and contains an exception that might be sufficient, in certain circumstances, to allow the EU to make commitments concerning cross-border flows of personal data in international trade agreements. Among other things, this thesis explores the tension between these two exceptions and examines various possibilities allowing for the objectives behind them to be met.

Not surprisingly in light of the above, the possibility of the inclusion of a provision on cross-border data flows accompanied by a GATS Article XIV-type exception for data protection in TiSA and TTIP<sup>58</sup> – both now stalled – sparked a strong push-back from European Parliament, academics and civil society in 2015-2016.<sup>59</sup> Later, in order to avoid

---

<sup>56</sup> See, e.g., Art. 28.3(2)(c)(ii) CETA; Art. 8.62(e)(ii) EU-Singapore FTA; Art. 167(1)(e)(ii) EU-Colombia-Peru FTA; Art. 7.50(e)(ii) EU-Korea FTA; Art. 203(1)(e)(ii) EU-Central America Association Agreement; Art. 135(1)(e)(ii) EU-Chile Association Agreement; Art. 23.1(2) KORUS; Art. 21.1(2) US-Singapore FTA; Art. 21.1(2) Dominican Republic-Central America-US FTA; Art. 21.1(2) US – Panama TPA; Art. 32.1(2) USMCA; Art. 29.1(3) CPTPP.

<sup>57</sup> CJEU, *Opinion on EU-Canada PNR Agreement*, paras 67, 70.

<sup>58</sup> See Le Roux (2017), p. 731 (‘The USTR includes an essential element that is still not addressed by the European Commission in its initial proposal, which is cross-border data flows. The United States thus remains very offensive on the matter and reproduced what they have already pushed through in the KORUS and the TPP texts’.) A bracketed draft for Article 2 of the Annex on Electronic Commerce to TiSA included a prohibition to ‘prevent a service supplier of another Party from transferring, accessing processing or storing information, including personal information, within or outside the Party’s territory, where such activity is carried out in connection with the conduct of the service supplier’s business’. Coalition For Privacy & Free Trade (2013) (‘The Obama Administration already has recognized the importance of interoperable privacy frameworks to global economic progress and prosperity: . . . The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation’.) But see Fontanella-Khan (2013) (noting EU officials’ fear that ‘finding a middle ground with the U.S. would only lower overall E.U. privacy standards’.)

<sup>59</sup> See e.g. Irion, Yakovleva, Bartl, pp. 44-45, 59-60; Fernández Pérez (2016); European Parliament resolution of 8 July 2015 containing the European Parliament’s recommendations to the European

any risk of undermining the fundamental rights to privacy and the protection of personal data, the EU ultimately refrained from including such a provision in the Economic Partnership Agreement between the European Union and Japan (JEFTA) and the revision of the EU-Mexico Free Trade Agreement.<sup>60</sup> In the case of Japan, the absence of such a clause was accompanied by the adoption of a mutual adequacy decision under the GDPR shortly before JEFTA took effect.<sup>61</sup>

In 2018, after a thorny interinstitutional dialogue, the EU developed horizontal provisions on cross-border data flows and the protection of privacy and personal data for its prospective digital trade agreements.<sup>62</sup> They include a specific exception for privacy and data protection, similar to the national security exception of Article XIV*bis* of the GATS – a text much broader than the above-mentioned general exception. Among other things, the proposed exception explicitly states that GATS-inconsistent measures for the protection of personal data and privacy are allowed, including rules limiting transfers of personal data. The EU has tabled these model clauses in digital trade negotiations ever since,<sup>63</sup> including into the EU proposal for the WTO rules on electronic commerce,<sup>64</sup> which are intended to co-exist with the general exception for privacy and data protection modelled after Article XIV(c)(ii) GATS included in the same agreement.<sup>65</sup>

Unlike the US approach to data flows, already implemented in CPTPP, USMCA and the US-Japan Digital Trade Agreement, the EU's approach in the above-mentioned 2018 model clauses contains a narrower prohibition on restrictions of cross-border data flows and a broader exception for domestic privacy and data protection rules.<sup>66</sup> Adherence to the US model by countries that maintain a free flow of personal data from the EU, in particular, Canada, Japan and New Zealand, puts pressure on the EU's restrictions on transfers of

---

Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)); European Parliament resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)).

<sup>60</sup> Both agreements include a commitment to reconsider the issue within three years after the agreement enters into force. See Art. 8.81 of JEFTA, Art XX of the Digital trade title of the Modernised EU-Mexico FTA. See also Fortnam (2017).

<sup>61</sup> European Commission, Adequacy Decision for Japan. Although this decision is commonly referred to as 'mutual', from a legal perspective it consists of two unilateral decisions adopted at the same time.

<sup>62</sup> EU model clauses on cross-border data flows; see also Aaronson, Leblond (2018) p. 262; Fortnam (2017).

<sup>63</sup> For an overview and discussion, see Section 4.2.

<sup>64</sup> Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce. Communication from the European Union. INF/ECOM/22, 26 April 2019.

<sup>65</sup> See e.g. Article X.1(2) of the EU proposal for Chapter X Exceptions of the EU-New Zealand FTA, 25 June 2019. This provision includes a general exception for privacy and data protection modelled after the general exception in the GATS Article XIV(c)(ii). EU proposals for Exceptions chapter for other trade agreements discussed in this thesis are not available as of the time of writing. For a discussion, see Section 4.2.2.

<sup>66</sup> For further discussion see Sections 3.3.4 and 4.2.1.

personal data. The EU is unlikely to agree to the cross-border data flow provisions such as those advanced by the US just mentioned above, for this would mean an unjustifiable derogation from EU Charter-based fundamental rights.<sup>67</sup> The clash between the US and the EU model is especially apparent in the Brexit negotiations between the EU and the UK, where the UK submitted provisions on cross-border data flows modelled after the US model,<sup>68</sup> while the EU submitted its model clauses as discussed above.<sup>69</sup> There is therefore an urgency to evaluate the EU proposal and see how much room the EU has to negotiate with the UK and other trading partners, assuming that the EU *should* continue to protect the rights to privacy and the protection of personal data as fundamental rights.

From an EU internal perspective, the EU's own framework for transfers of personal data has been criticised on multiple occasions for its broad reach and insufficient and inconsistent enforcement.<sup>70</sup> An important prerequisite of developing an alternative framework, however, is a deeper understanding of the relationship between Articles 7, 8 and 52(1) of the EU Charter and the GDPR, and the extent to which the EU legislator is free to design the framework for transfers of personal data without overstepping constitutional boundaries. This issue ties into a broader ongoing academic debate on the essence of the EU fundamental rights and the relationship between EU primary and secondary law.

## 1.2 Research questions and methodology

The main 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 this question in four steps by addressing the following four sets of sub-questions, relating to (1) compatibility, (2) protectionism, (3) reconciliation, and (4) reform of the EU restrictions.

1. *The compatibility question.* Are the primary obligations of the GATS and EU restrictions on transfers of personal data outside the EEA compatible, and if not, can this incompatibility be remedied by the application of the general exception in the

---

<sup>67</sup> This is because, as explained in Section 2.3.4, the trade 'necessity test' that lies at the heart of the exception for privacy and data protection in US-led trade agreements requires a derogation from fundamental rights beyond the limits set by Article 52(1) of the EU Charter.

<sup>68</sup> Arts. 18.13 and 18.14 of the Draft Working Text for a Comprehensive Free Trade Agreement Between the United Kingdom and the European Union, Draft UK Negotiating Document.

<sup>69</sup> Draft text of the Agreement on the New Partnership with the United Kingdom, European Commission, 18 March 2020, p. 135.

<sup>70</sup> For a discussion, see Section 5.3.

GATS and Article 52(1) of the EU Charter?

2. *The protectionism question.* Do EU restrictions on transfers of personal data outside the EEA constitute protectionism? Where should the line be drawn between protection and protectionism? What roles do more general discourses play in determining what amounts to legitimate protection and what to illegitimate protectionism? How does framing the debate on privacy and data protection in terms of ‘digital protectionism’ affect the normative foundations of domestic regulation on privacy and personal data, and setting appropriate levels of privacy and personal data protection?

3. *The reconciliation question.* Do the model clauses proposed by the EU for digital trade chapters meet the EU’s ambitions of reconciling cross-border data flows under international trade law with the protection of the rights to privacy and personal data as fundamental rights under the EU Charter, whilst maintaining a global rules-based trading system? If they do not reconcile, then what are the issues preventing them from doing so? Are there other ways in which the two policy objectives can be reconciled?

4. *The reform of the EU restrictions question.* What are the weaknesses of the EU framework for transfers of personal data outside the EEA from the EU Charter perspective, and how can they be addressed in a manner both compliant with the EU Charter and conducive to international trade? Do restrictions on transfers of personal data outside the EEA constitute part of the essence of the fundamental right to privacy, to the protection of personal data and to an effective remedy?

Turning to methodological questions, for the most part, the research question calls for a doctrinal analysis of the law from an internal perspective.<sup>71</sup> The main research question is evidently normative, asking how competing values and interests *should* be reconciled. The first normative basis will be the law, even if it will become evident that the law—as an expression of such competition—will not give away the answer.

The thesis thus engages first of all in an argument about what the law is, with a view towards developing it further.<sup>72</sup> This approach is necessary in order to inform the legal arguments in this thesis. First, it engages with the reform of the international trade exception for privacy and data protection in future EU trade agreements. And second, with the reform of the EU framework for transfers of personal data outside the EEA under the

---

<sup>71</sup> Smits (2012), p.3 (defining the doctrinal method as ‘approach, in which rules, principles and case law are considered from the internal perspective and in which law is looked at as being in a relatively autonomous relation to the social, economic and political reality’.)

<sup>72</sup> Von Bogdandy (2009), p. 377.

GDPR in a manner respectful of EU fundamental rights.<sup>73</sup> The doctrinal analysis systematises the legislation and jurisprudence of the CJEU and the WTO adjudicating bodies within the scholarly schemes established in secondary literature from the relevant legal domains, in particular, EU law, European data protection and international trade law.<sup>74</sup> For example, Chapter 2 of the thesis uses close reading of the relevant legal provisions of the GATS and the GDPR, in the light of their interpretation in the CJEU and WTO jurisprudence and secondary literature, to analyse and compare the necessity tests in the EU Charter and in the general exception of trade agreements, modelled after Article XIV GATS. Chapter 4 deconstructs the text of the EU model clauses on cross-border data flows and examines each element of these clauses by comparing it to the existing legal provisions as interpreted in the relevant WTO jurisprudence and secondary literature. Chapter 5 applies the same methods, amplified by an emphasis on the existing legal practice, to evaluate the EU framework for transfers of personal data in the GDPR and to explicate the relationship between the EU Charter and the GDPR in the context of the governance of transfers of personal data outside the EEA.

In order to further support its normative argument, the thesis complements the classical doctrinal method by a historical approach to law,<sup>75</sup> elements of economic analysis of law, and critical legal studies.<sup>76</sup> The interplay between these methods plays a central role in the development of the arguments in Chapter 3, addressing the question of where to draw a line between protection and protectionism, and how the framing of the debate on trade and data privacy affects the degree of regulatory autonomy afforded to domestic privacy and data protection rules. Relying on the literature on economics and the political economy of international trade, Chapter 3 takes a historical perspective to trace how the notion of ‘protectionism’ has evolved over time. The discussion of the role of discourse in shaping the meaning of ‘protectionism’ is also informed by the literature on language and power, which falls under the umbrella term of ‘discourse analysis’. It then applies these insights to the current debate on whether, and to what extent, EU restrictions on transfers of personal data outside the EEA can be viewed as protectionist. The discussion of the dual nature of personal data in Chapter 3 requires a conceptual analysis of personal data, which contraposes its dignitary and economic aspects. An understanding of both the economic nature and life cycle of personal data rests on an external, essentially economic approach. Juxtaposing the legal and economic perspectives on the protection of personal data allows the thesis to put the tension between the two approaches in sharp contrast. This tension

---

<sup>73</sup> Hervey, Cryer, Sokhi-Bulley, Bohm (2011), p. 34ff; Van Gestel, Micklitz, Maduro (2012), p. 2; Vermeule (2007), p. 394–395.

<sup>74</sup> Von Bogdandy (2009), p. 377.

<sup>75</sup> Handler (2013).

<sup>76</sup> Finnis (2011).

translates into conflicting goals and differing notions as to the right level of regulation, depending on whether personal data is protected as an economic asset or a fundamental right. This part of the discussion draws on the academic literature informed by a law and economics theory of regulation, which addresses regulation from an economic efficiency standpoint.<sup>77</sup> By contrast, a discussion of the dignitary aspect is based on the academic literature embracing a moral and legal approach reflecting the value attached to personal data by international human rights and EU law.

There is a variety of international trade agreements that go a step further than the WTO agreements in regulating issues related to electronic commerce and data (WTO plus agreements).<sup>78</sup> In analysing the governance of cross-border data flows, the thesis takes an EU perspective, which it juxtaposes with that of the US. For this reason, the scope of WTO plus agreements considered in this thesis is limited to the recent EU-led, already-concluded or draft trade agreements and proposals for trade agreements currently negotiated by the EU: JEFTA, draft Modernised EU-Mexico Free Trade Agreement (FTA), the EU's proposals for FTAs with Australia, Indonesia, New Zealand, Tunisia and the UK. The above-mentioned proposals for trade agreements are relevant for the analysis in this thesis because they contain specific provisions on cross-border data flows. Bringing JEFTA and the draft EU-Mexico agreements into the discussion gives a historical perspective to the debate on cross-border data flows in the international trade realm. On the US side, the analysis in this thesis includes the already mentioned CPTPP, USMCA and the US-Japan Digital Trade Agreements, which are the only US-led trade agreements that contain a legally binding provision on cross-border data flows. The US model has been chosen as a point of comparison with the EU model, for the reason that it is currently the most influential model which is incorporated in currently concluded international trade agreements. For example, as mentioned above, the UK has adopted the US rather than the EU approach to cross-border data flows in Brexit negotiations with the EU. In the data protection realm, the issue of transfers of personal data from the EEA to the US has been one of the most contentious within the lifetime of the EU data protection framework. The focus on the EU-US relationship, however, does not diminish the fact that the balancing of economic, fundamental rights and other policy objectives in the governance of cross-border data flows is a global issue.

This thesis does not engage with the debate on the classification of goods and services when it comes to cross-border data flows.<sup>79</sup> The focus of this thesis is on international agreements covering trade in services and electronic commerce, which is

---

<sup>77</sup> Ogus (1994), pp. 23-54.

<sup>78</sup> For a most recent overview of such provisions, see Burri, Polanco (2020).

<sup>79</sup> For a discussion, see e.g. Sen (2018), p. 330-335.

referred to as digital trade in most recent trade agreements. The thesis does not cover trade in goods, even though in some cases, measures restricting data flows could be targeting ‘goods attributes’ of a product, such as an Internet of Things device.

It should also be acknowledged that approaching cross-border data flows from an international trade perspective, as adopted by this thesis, is only one way of looking at freedom of information flows more generally. In a broader context, restrictions on data flows implicate other policy objectives, such as freedom of speech, as well as (international) media and communications freedom, which, in a wider sense support political, social and economic activity. As Mueller and Grindal rightly observe, the economic value of data flows is a ‘by-product of the social, communicative and productive capability caused by untrammelled information flows’.<sup>80</sup>

### **1.3 Outline of the thesis**

The Chapters of this thesis tackle in turn the research sub-questions posed above. Chapter 2 explicates the EU restrictions on transfers of personal data outside the EEA against the background of the concerns that led to the emergence of the EU data protection framework in the 1990s. It then demonstrates the possible tension between these restrictions and existing EU international trade commitments, especially under the GATS. The Chapter further argues that there is a risk that this tension cannot be ameliorated by the application of exceptions provided for in EU and trade law, due to the incompatibility of these exceptions when applied simultaneously. Put simply, Chapter 2 sets out the main issue addressed by this thesis: the conflict between commitments to data protection, and trade liberalisation.

Chapter 3 takes a step back and investigates whether EU restrictions on transfers of personal data outside the EEA are protectionist. One could argue that the balance between digital trade liberalisation and the protection of data privacy should simply be struck by ruling out measures that are protectionist in nature. The problem is, however, that the baseline between legitimate protection and protectionism does not exist. Chapter 3 investigates how views on this baseline are discursively constructed and how this baseline has shifted over time. The Chapter demonstrates how discourse affected the conceptualisation of the notion of ‘protectionism’ in international trade negotiations and WTO case law, and translates these findings into a number of recommendations for future international trade negotiations on digital trade and cross-border data flows. Chapter 3 also shows how discourse can affect the normative foundations of the public policy objectives incorporated into trade law exceptions, such as privacy and the protection of personal data,

---

<sup>80</sup> Mueller, Grindal (2019), p. 82.

and, as a result, the level of protection of such objectives in domestic legal systems.

Chapter 4 turns to the international trade law aspect of the problem identified in Chapter 2. It questions whether the model clauses on cross-border data flows and the protection of personal data tabled by the EU in all trade negotiations on these issues would allow the EU to resolve that problem whilst maintaining its trade policy objectives. Having identified the weaknesses of the model clauses, Chapter 4 looks for alternatives.

Chapter 5 examines the weaknesses of the EU framework for transfers of personal data outside the EEA from the EU Charter perspective and asks how this framework could be improved to ameliorate the problem identified in Chapter 2. It examines this framework through the lens of geopolitical, legal and economic changes, and the constitutional function of those rules in order to establish whether this framework is still fit for purpose or needs to be improved. Engaging with the idea of future reform, Chapter 5 addresses the relatively unexplored issue of the constitutional contours of EU secondary law framework for transfers of personal data. Relatedly, it explores the flexibility that the EU legislator has under the EU Charter to change the rules of the GDPR on transfers of personal data. It also provides three directions of thought on future reform, roughly corresponding to possible short, medium, and long term strategies for the EU.

Chapter 6 offers conclusions structured as responses to the research questions formulated above and envisions paths for further research.

Research in this thesis is up-to-date until *1 September 2020*. After that only a small number of substantive additions and changes have been made. Some parts of this thesis are based on the author's published work. In particular, Chapter 2 is based on S. Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, *Journal of World Investment & Trade* 21 (2020) 881–919; Chapter 3 is based on S. Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, *University of Miami Law Review*, 74 (2) (2020) 416-519. This thesis also cites individual and co-authored work that preceded and paved the way to this thesis.