The Landing Zone in Trade Agreements for Cross-Border Data Flows

Dr. Pascal Kerneis[1]

Working Paper No. 2021-12

Author Bio

Dr. Pascal Kerneis holds a Ph.D. in European Law from the University of Rennes, France. He held the position of Legal Expert with the European Commission in Brussels from 1988 to 1990, and then worked for the European Banking Federation as International Affairs Adviser. In 1999, he was appointed Managing Director of the European Services Forum (ESF), the voice of the European services industry in international trade and investment negotiations. Dr. Kerneis has also took on the role of Special Advisor to Business Europe International Affairs Department in 2010-2012.

Pascal Kerneis is a long-standing member of the DG Trade Civil Society Contact Group. He participates in all the European Domestic Advisory Groups (DAG) set up for the EU FTAs, and chairs the EU-Singapore DAG established in 2020. He has participated in all WTO Ministerial Conferences as an advisor to the Commission. In 2014, he was appointed to the Commission's Advisory Group for the Transatlantic Trade and Investment Partnership (TTIP) with the United States. In 2017, he was appointed to DG Trade's Expert Group on Trade Agreements. He is a regular public speaker on trade and investment in services and an active author of multiple contributions to academic books and publications.

Citation

Kerneis, P. 2021. "The Landing Zone in Trade Agreements for Cross-Border Data Flows", Jean Monnet Network TIISA Working Paper No.2021-12, September, 2021.

Trade and Investment in Services Associates (TIISA) Network

Co-funded by the Erasmus+ Programme of the European Union

[1] The views expressed herein are those of the author and do not necessarily reflect an official position of the European Services Forum (ESF).

Table of Contents

1. Introduction

The digitalisation of the world economy is continuing at a fast pace. Its successful progress is dependent on the ability to move data as freely as possible across international borders. Digital Trade Chapters are therefore becoming an ever more important and critical part of bilateral, plurilateral and multilateral trade agreements. Various domestic policy objectives are defended by trading partners, which lead to differences in approaches to regulating cross-border data flows. This paper explores where a landing zone might be found that would allow adoption of global rules on electronic commerce (e-commerce) and digital trade.

We first aim to explain the background historical context. We then look at the specific issue of cross-border data flows in various negotiating camps and examine divergences and similarities that might lead to an acceptable solution for international rules on digital trade.

2. Understanding the Historical Context

2.1 The multilateral background

The WTO Uruguay Round ended 25 years ago when the internet was still in its infancy. But global rules on digital trade have not been updated since.

In 1998, WTO members adopted the Reference Paper on Basic Telecommunications, which sets rules for that sector, but does not include the "value-added" telecommunications services which compose the bulk of todays' digital services trade and cross-border data flows. Moreover only 82 WTO members have effectively included the Reference Paper via "additional commitments" in their GATS schedules and are hence bound to respect the regulatory principles therein.

At the 2nd WTO Ministerial Council in May 1998, Ministers, recognising that global e-commerce was growing and creating new opportunities for trade, adopted a Declaration on Global Electronic Commerce. This called for the establishment of a work programme on e-commerce, which was adopted in September that year. Periodic reviews of the programme are conducted by the WTO General Council based on reports from the WTO bodies responsible for implementing the programme. Ministers also regularly consider the programme at the WTO's Ministerial Council Meetings. Ministers also agreed to continue the practice of not imposing customs duties on electronic transmissions until their subsequent session. After repeated extensions at subsequent sessions, this Moratorium is now under question by some WTO members, who consider they are losing some possible revenue.

It is in that difficult context of blockage and division in the WTO run by the consensus rule, that many Members decided that a new path was necessary. They decided at the 11th WTO Ministerial Council in Buenos Aires, Argentina in December 2017, to propose to those Members which were willing, to support a so-called "Joint Statement Initiative" (JSI) on E-Commerce. That initiative launched exploratory work towards future WTO negotiations on trade-related aspects of e- commerce, with participation open to all WTO members. 71 Members joined this initiative.

The work is going on and many rounds of talks, plenary and small group meetings are regularly taking place in Geneva. 86 Members are now part of the initiative, representing more than

80% of global trade in services. Progress has been made on some important issues with legal text for future rules nearly closed, for example on e-signatures, e-authentication and anti-spam etc. Other text proposals are on the table on issues such as open government data, online consumer protection, paperless trading, open internet access, source code protection, e-contracts, customs duties on e-transmissions and transparency. All of that is well and good and needs to go further, hopefully with a clear report on the progress made at the 12th Ministerial Council in November 2021 in Geneva, including a clear timeline towards completion.

But negotiators have not yet touched upon the decisive issue which would really impact global rules on digital trade: the issue of cross-border data flows (CBDF). This is the most contentious issue and will be dealt with only at the very end. We look further at that matter in Section II of this Paper.

2.2. The bilateral/plurilateral path

a) CP-TPP & affiliated

In the absence of rules at the multilateral level, many WTO members have felt the need to enact some rules for the flow of data between them. This can be done through the bilateral or plurilateral route. The first ever agreement with a complete chapter on digital trade was the Comprehensive and Progressive agreement for Trans-Pacific Partnership (CP-TPP), that gathers 11 countries, signed in March 2018 (**Australia**, **Brunei**, **Canada**, **Chile**, **Japan**, **Malaysia**, **Mexico**, **New Zealand**, **Peru**, **Singapore**, and **Vietnam**). But the rules of the agreement, and in particular of the digital trade chapter, were negotiated and signed in February 2016 among a group of 12 countries that included the **United States of America (USA)**, which finally opted-out of the deal, but having had a significant negotiating influence on the content of the chapter.

The United States–Mexico–Canada Agreement (USMCA) came into effect on 1st July 2020, but negotiations were finalised in principle in October 2018. The Digital Trade chapter takes the E-Commerce Chapter of CP-TPP as a basis, and improves it, notably by covering financial services. After CP-TPP, Australia negotiated an FTA with Hong Kong, China and that text on CBDF also includes financial services (entering into force on 17th January 2020).

In October 2019, the USA and Japan signed the U.S.-Japan Digital Trade Agreement, which entered into force on 1st January 2020. It establishes high-standard rules in this area, demonstrating the willingness of both countries to maintain a leading role in global rulemaking on digital trade. It is the first agreement that legally binds the USA on the full gamut of digital trade rules, closely followed by USMCA.

Among the CP-TPP signatories, some parties considered that the text on digital trade was not going far enough, and decided to adopt even deeper rules on digital trade among themselves. This was the case between Chile, Singapore and New Zealand which concluded the Digital Economy Partnership Agreement (DEPA) in June 2020. The DEPA, which entered into force in December 2020, is a first of its kind agreement that establishes new approaches and collaborations on digital trade issues, promotes interoperability between different regimes and addresses the new issues brought about by digitalisation. This was followed by the Australia-Singapore Digital Economy Agreement (DEA) signed in March 2020 and entering into force on 8th December 2020. The DEA upgrades the digital trade arrangements between Australia and Singapore under the CP-TPP and the Singapore-Australia Free Trade Agreement – which are already among some of the most ambitious agreements globally. For example, the DEA delivers more robust rules that ensure businesses, including in the financial sector, can transfer data

across borders and will not be required to build or use data storage centers in either jurisdiction. It improves protections for source code; establishes new commitments on compatible e-invoicing and e-payment frameworks; and delivers new benchmarks for improving safety and consumer experiences online.

We recently learned that the UK and Singapore have formally launched negotiations towards a Digital Economy Partnership Agreement (June 2021). This is happening at the same time that the UK is negotiating to join the CP-TPP and nearing completion of its FTA negotiations with both Australia and New Zealand. The UK Government is also talking about how a future USA-UK free trade agreement can "set gold-standard rules" on digital trade. In addition, in June 2021, Australia announced it was in talks with the USA. about a possible digital trade agreement, with the hope that negotiations will result in a regional agreement "so that America, Australia, Singapore, Japan and others can set the rules and standards in the region." Furthermore, Korea (which is not part of CP-TPP) is negotiating to join DEPA.

It is important to note that all these agreements include language asserting the principle of freedom of cross-border data flows.

This group of dynamic countries, which are working towards developing global rules, is however only regrouping the same fourteen countries. That is hardly "global". So, what about other countries or groups of countries?

b) EU FTAs and e-commerce/digital trade sections

The European Union (EU) has negotiated an "Electronic Commerce" chapter in its agreement with **Canada**, which entered into force (provisionally) in September 2017, but that was negotiated in 2014. Chapter 16 of the Comprehensive and Economic Trade Agreement (CETA) between EU and Canada has provisions to enhance trust and confidence in e-commerce, to protect personal information on the internet and to ensure that online services are not subject to customs duties. But there is no provision on CBDF.

The EU-**Singapore** FTA that was signed in October 2018 and entered into force in November 2019 includes a chapter on E-Commerce (Chapter 8), but it was also negotiated in 2013 and does not have any provision on CBDF.

The EU has a chapter on E-Commerce in its FTA with **Japan** that entered into force on 1st February 2019 (Chapter 8). The chapter goes a bit deeper with provisions on combatting unsolicited messages, on consumer protection, on e-authentication and e-signature, on protection of source code, etc. But there is a three-year review clause to reassess the need for incorporation of provisions on the free flow of data into the agreement (Article 8.81).

The EU and **Vietnam** signed a Trade Agreement and an Investment Protection Agreement on 30 June 2019. The Trade Agreement entered into force on 1st August 2020. One might expect that the digital trade chapter would be forward-looking, given that Vietnam is a signatory to CP-TPP. But, on the contrary, the E-Commerce chapter (Chapter 8 – Section F) is very weak with basically no obligations apart from banning customs duties on e- transmissions. It is worth noting that the negotiations were finalized in December 2015.

One of the most recent agreements the EU has reached in principle is with the four countries of **Mercosur** (Argentina, Brazil, Paraguay and Uruguay). The deal was announced on 28 June 2019 after twenty years of negotiations. Sub-Section 6 of the Title on Services and Establishment deals with e-commerce, and is quite similar to the text signed with Japan. The

three-year review clause applies to the whole chapter. This agreement is not yet ratified and implemented.

The EU and Mexico have reached an "agreement in principle" on the main trade parts of a new EU-Mexico Association Agreement. The new agreement will replace a previous bilateral deal dating from 2000. Negotiations with Mexico started in May 2016 and both sides reached an agreement in principle on the trade part in April 2018. Other aspects of the deal still need to be finalised, however, before going to ratification. This agreement is the EU's first agreement that has a chapter entitled "Digital Trade". The text goes into more detail in many articles, but at the time of negotiation, the EU was still not ready internally (see below) and hence includes only a review clause on CBDF, like the one with Japan.

The only free trade agreement implemented by the EU which enacts rules on CBDF is also the most recent and probably the most forward-looking FTA ever signed by the EU. It is the EU-UK Trade and Cooperation Agreement (EU-UK TCA) that was signed after the exit of the United Kingdom (UK) from the EU on 30 December 2020. It applied provisionally from 1 January 2021, when the Brexit transition period ended, before formally entering into force on 1 May 2021. Digital trade is not a section of the Services and Investment chapter as in other EU FTAs but has a fully fledged Title (Title III – from Article 196 to 212). Chapter 2 of that title is labelled "Data Flows and Personal Data Protection". We will return to that specific chapter later in the paper.

Finally, the EU is currently negotiating FTAs with Australia and New Zealand. The negotiations of these agreements are well advanced, and conclusions might be envisaged in the course of 2021/22. Discussions on the digital trade chapter are tense, as the two Pacific countries are requesting that the EU adopt language similar to the rules that apply through the CP-TPP, and indeed accept further provisions as they agreed with Singapore and Chile in their DEA or DEPA. For its part, the EU is willing to find a compromise that takes its concerns on personal data protection into consideration.

The final result of these digital trade chapters, in particular with Australia, might demonstrate what could be a possible landing zone for global trade rules on CBDF (through the WTO JSI on E-Commerce).

It is interesting to note that all countries with which the EU has agreed or is negotiating an e-commerce/digital trade chapter are all members of (or willing to accede to) the CP-TPP, except Mercosur.

3. What are the different strategies to manage cross-border data flows?

One can identify three groups of countries with three different strategies on CBDF that reflect their respective fundamental values and practices in governing societies.

- The first group traditionally put the emphasis on business priorities in managing digitalisation of the economy and trade;
- The second group puts the priority on people and citizens, so data can flow as freely as possible but with proper protection of privacy, set as a fundamental human right;
- The third group puts priority on the role of government in managing the flow of data, so as to ensure national security and protection of citizens.

3.1 The US and CP-TPP: assertion of the principle of free flow of data for development of the digital economy

As for any innovation, business adoption of digital trade practice is well in advance of governments and regulatory bodies. When e-commerce started to cross borders, the basic standards were set by the companies running the new innovations and services around them. And this circle continues with new start-up companies coming into the world market on a daily basis, with, by definition, no trade rules in place for their new business offerings. In the USA, and in the CP-TPP countries, governments tend to consider that as little intervention as possible in this kind of business, like in many other sectors, is the best way to spur digitalisation of the economy, which in turn creates wealth, jobs and more innovation, benefitting the country and the whole global economy. They consider therefore that the rules governing digital trade should respect the principle of freedom of CBDF, which can however be subject to some exceptions, like national security and "legitimate public policy objectives".

3.2 The EU and the issue of personal data protection

In the EU, the priority for European society, and hence EU Member government action, is not based around the economy, but around the central role of human activities as a whole. The economy and international trade are tools to improve the human condition. And to enhance the human condition, society must respect fundamental values that must be reflected in all activities. And, related to digital trade, one of the fundamental values is respect for the personal data of all citizens.

Why postpone provisions in EU trade agreement on CBDF? The whole issue was blocked for a long time by the internal process within the EU of debate over personal data protection. We need to remember that the EU had already been unable to move forward on the matter of CBDF in the Trade in Services Agreement (TiSA) negotiations, which were launched in March 2013 and finally collapsed in November 2016, a few weeks after the election of USA President Trump. The EU was unable to take a position on how to reconcile strong personal data protections as clearly demanded by European citizens (*see below*), with the need to ensure free flow of data across borders to accompany fast development of digitalisation of the European and global economy.

The EU was and still is concerned that too liberal a text in an international treaty, being bilateral, plurilateral or multilateral, could allow some signatories to question, through a dispute settlement mechanism, the validity of the EU's internal provisions on data protection, and in particular, its flagship legislation adopted in April 2016 and called the General Data Protection Regulation (GDPR), which entered into force in May 2018.

It is useful to remember the context. Protection of personal data has always been a key concern of European citizens due to the continental history (2nd World War, cold war, etc.). The EU had already adopted a Data Protection Directive in December 1995, when the internet was at its very beginning. European citizens had already from the start of the digital age tended to a negative suspicion that their privacy could be endangered by this new technology.

It is worth remembering that the WTO General Agreement on Trade in Services (GATS) was negotiated during this same period, entering into force in January 1995. The EU managed to introduce into the text of the "general exceptions" (GATS Article XIV) a possibility for a Member to adopt a measure "c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this agreement including those related to (ii) the protection of the privacy of individuals in relation to the processing and the dissemination of personal data and the protection of confidentiality of individual records and accounts".

The EU was in the process of updating the Directive of 1995 when the "Snowden scandal" came up in June 2013, revealing that foreign surveillance authorities were spying extensively on European citizens' data, all the way up to German Chancellor Merkel. It was also the period when activist Julian Assange, WikiLeaks founder, was regularly feeding related leaked stories to the media. These events had a very significant impact on European societies. All of these factors exacerbated the debate in the EU institutions which pushed for even stronger regulation to protect the personal data of EU citizens. This led to the famous GDPR, which requires all companies (from within the EU and from outside the EU) wanting to obtain access to EU consumers' data (in the process of an e-commerce transaction for instance) to respect a high degree of personal data protection.

It was only after fierce debate within the European Commission, within the European Parliament, and within the European Council of Ministers, and between all these institutions, and only when faced with the need to move on this issue, that finally a compromise was found in February 2018. Under the compromise, the EU could accept strong language on cross-border data flows in trade agreements, with strong provisions banning localisation requirements, but also with a very strong provision allowing parties to set safeguards they deem appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data.

This last requirement would allow the EU or its trading partners signatory to such a provision to enact barriers to cross-border data flows, including imposing localisation requirements, for the sole purpose of personal data protection. Many countries, in particular the USA and the 11 CP-TPP countries, consider this carve-out much too broad and therefore resist such a provision.

3.3 Control of data flows by governmental authorities (China, Russia & other countries)

Another group of countries take a different approach to cross-border data flows. They consider that the government must have the main role in regulating the whole society to ensure its safety, security and prosperity. Therefore, as for many other aspects of life, the government wants to control flows of data in the country and coming into and going outside the country.

These countries tend to impose on companies that want to do business with their countries requirements to localise data processing or data storage in the territory of the country and subject the flow of data across borders to controls and restrictions. These localisation requirements can be a tool to oblige digital companies to set up a joint venture with a local business, which might then benefit from technology transfer, while the country would benefit from job creation by this new part foreign-owned establishment.

This tends however to be short-sighted strategy, as this data protectionism has the counter-effect. Inward foreign direct investors that are forced into local partnership are generally less efficient, with higher cost structures, and keep technology transfers limited to the minimum. When investors are free to keep control of their management and of the flow of data, investment is more massive, hence the creation of jobs and the natural transfer of know-how through the mobility of workers and data are more effective.

Furthermore, some countries will opt for this policy approach of controlling the flow of data as a means of controlling the society. This can be the case for instance with measures which control the internet and the media. Other ways to control data moving from foreign companies is through censorship, and through granting of licenses to operate only on obtaining access to

the source code of software and programmes operated by these firms. These practices are clearly in total conflict with the free flow of data policy or with the policy of flow of data that respects human rights (including personal data protection).

4. Is it possible to adopt Global rules for cross-border data flows?

Taking into account these three groups of countries and their different ways of governing cross-border data flows, let's explore whether it will be possible to agree on some sets of global rules.

4.1 A first nexus of global rules

There is clearly a central nexus of rules to which the governments that have decided to join the Joint Statement Initiative on E-Commerce will hopefully be ready to commit. This minimum set of rules for a WTO agreement on E-Commerce will fix global rules for issues like e-signature and e-authentication, anti-spam, online consumer protection, paperless trading, electronic contracts, ban of customs duties on electronic transmissions, transparency of regulatory framework, etc. The implementation of all these rules will be a great achievement and will undoubtedly improve the legal environment for development of digitalisation of the economy, including in many developing countries. It should therefore contribute in narrowing the digital divide. The whole question will be whether it would be of sufficient interest to those WTO members, which would like to go further by setting rules on cross-border data flows, to sign up to such a restricted agreement.

Indeed it will probably be even more difficult to gather a large consensus on other important issues such as open government data, open internet access, source code protection, ban of localisation requirements, personal data protection, improved rules on telecommunications services and value-added related services and improved market access commitments in services sectors related to digital trade, etc.

Efforts will be made to push for a better deal, but it seems clear that not all JSI participants will be willing and able to put into question the way they manage the flow of data in their own territory. So, at a point in time, decisions will need to be made on whether there is no deal at all because it is not sufficiently ambitious - or whether there will be a deal with as many issues acceptable to as large a group of WTO members as possible. That deal could serve as a first nexus of global rules. The ideal would be that it will indeed be an agreement that will cover the whole WTO membership on the basis of the Most Favoured Nation (MFN) principle. But, if that would not appear feasible, a plurilateral agreement between all the current 86 participants in the JSI on E-Commerce should nevertheless be concluded. It would demonstrate that the WTO is capable of adapting itself to new conditions. It will show that the negotiating function of the WTO is still able to deliver on an issue related to the modern economy, and hence remains relevant. The agreement should remain open to other WTO members, and indeed include a review clause.

4.2 Stronger rules for the group of the willing?

It might then be envisaged, that a group of countries of the willing will decide to pursue negotiations on the remaining issues, such as those mentioned above.

Going back the various groups of countries analysed earlier in this paper, one can assess that only the first two groups will participate in these on-going negotiations. We are therefore

talking about the USA and the eleven countries of the CP-TPP, and the 27 members of the EU, to which one can add the UK, Norway, Iceland, Liechtenstein and Switzerland. One can also add WTO members that are not part of these two groups but are active in pushing for more digital trade rules for example Colombia, Costa Rica, South Korea, Panama, Chinese Taipei, and maybe a few more, such as Georgia, Moldova and Ukraine. That would assemble a group of around 50 WTO members, representing more than 60% of global trade.

Where might such negotiations lead? What are the issues that will readily gather consensus, and which will be more problematic?

Looking at the various FTAs that have been agreed by these WTO members *(see Section I here above)*, one can identify subjects that should be acceptable to most of them, like open government data, open internet access, source code protection, ban of localisation requirements. The matter of personal data protection is tackled in nearly all FTAs, but perhaps not in terms that would be acceptable to all. So, some fine-tuning will be necessary.

Other issues like improved rules on telecommunications services and value-added related services, improved market access commitments in services sectors related to digital trade, are not yet gathering much support. Will the supporters of such rules and better market access insist on agreement on those aspects in order to cross the finishing line in this smaller group of the willing? This remains to be seen, and much will depend on the moves that might be agreed on other issues just mentioned (free flow of data, ban of localisation requirements, personal data protection, etc.)

There is one issue that has not attracted much debate, but that will require a solution for the negotiations to go ahead. This is the issue of "non-discrimination of digital products" that is an article in the CP-TPP, the USMCA and the US-Japan Digital Trade Agreement.

A. Non-Discriminatory treatment of digital products

Article 19.4 of USMCA states that

> *"1. No Party shall accord less favourable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products."*

It is very important to note paragraph 2 that states:

> *"2. This Article does not apply to a subsidy or grant provided by a Party, including a government-supported loan, guarantee, or insurance."*

At the beginning of the digital trade chapter, one finds the definition of digital products.

> *"Digital product means a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. For greater certainty, digital product does not include a digitized representation of a financial instrument, including money".*

The problem here lies in the fact that the EU does not recognise data transmitted electronically as "products". They are considered to be services. This classification has significant potential impact. This distinction first arose during the Uruguay Round negotiations, during which the USA wanted to negotiate zero tariff and zero quota outcomes on these "products" including the audio-visual production of film, TV programmes, etc. The EU members wanted to be able to continue to provide subsidies for the production of films, sound recordings, etc, with the

objective of protecting cultural diversity. This policy had first been put in place at EU level in October 1989 with a first Directive [2] on audio-visual services. It creates quotas where a determined minimum of local production has to be programmed by cinemas and TV channels. Progressively, with the growing digitalisation of these productions that could be transmitted electronically, the EU regulation was imposing discriminatory treatment on these "digital products". The EU always argued that the electronic versions of audio-visual productions were not products but services. Moreover the EU has always excluded audio-visual services from its Services Chapters of international trade agreement.

What was at stake here was the survival of local European production of audio-visual content. The heavy insistence of the US film industry on removal of all trade barriers to further penetrate the EU market in the 1990s, while it already had around 80% of the market for film distribution, triggered a massive social movement on the part of the French and European film industry and workers (actors, film makers, celebrities) seeking protection, and gaining popular and political support. The EU did not want to close its market to foreign films (as the market was indeed already relatively open and indeed dominated by non-EU films) but wanted to be able to protect its own production in the interest of promoting cultural diversity.

When the GATS came into force in 1995, the EU did not take any commitments in its schedule on audio-visual services. But it remained the case that, possibly at the next occasion of services negotiations – scheduled to commence in five years according to Article XIX of GATS (i.e. in 2000) – the pressure could be expected to come back and the sector would again have to lobby to maintain the exclusion. The sector therefore worked with European authorities to find another route of protection. The outcome was the adoption of the Universal Declaration on Cultural Diversity of 2001, which then led to adoption of the UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions, which is a binding international legal instrument, by the UNESCO General Conference on 20 October 2005.

But given the strong dispute settlement of the WTO (at that time!), the audio-visual sector felt that the protection provided by the UNESCO Convention might not be enough. It therefore worked together with some European governments on a second track of protection, related to EU trade policy, and looked at a full and definitive exclusion. That led to the adoption of the Article 207 of the Treaty on the Functioning of the European Union (TFEU), known as the Lisbon Treaty signed on 13 December 2007 and entering into force on 1 December 2009. It states in paragraph 4

> *"The [EU] Council shall also act* ***unanimously*** *for the negotiation and conclusion of agreements: (a) in the field of trade in cultural and audiovisual services, where these agreements risk prejudicing the Union's cultural and linguistic diversity; (…)."*

Given that it would be extremely difficult to get unanimity of all EU governments, this means that a change of EU policy on that matter would now require a change in the EU Treaty, which is highly unlikely in the near future.

Therefore, should a group of countries decide to go ahead with a plurilateral Digital Trade Agreement in which they want to include an article on digital products, it is likely that the EU27 will not be able to join.

---

[2] *Council Directive 89/552/EEC of 3 October 1989, amended many times and repealed by Directive 2010/13/EU of 10 March 2010 (Audiovisual Media Services Directive), itself amended by Directive (EU) 2018/1808 14 November 2018*

One can wonder at this point what the real problem is for the EU. If the words "digital product" is the main concern, then the EU could maybe propose to set the definition of "digital product" to suit its views, or choose a different expression e.g. "digital service". If the real problem is a ban on discrimination against "digital products" then it might need to be clearly expressed. CP-TPP signatories will argue that their commitment is a ban on discrimination between the digital form and the analogue or hard copy form, and therefore a ban on technological discrimination. And it is precisely because the EU wants to be able to continue to discriminate in favour of its own/EU produced audio-visual services or products, that it cannot make such a commitment.

One of the questions that the participating parties will have to assess before taking a stance on this issue is what the real value of such a provision is. As mentioned earlier, paragraph 2 of Article 19.4 of USMCA states that the non-discriminatory treatment of digital products

> *"does not apply to a subsidy or grant provided by a Party, including a government-supported loan, guarantee, or insurance".*

This means that the USA, Canada or Mexico can provide subsidies to their own digital products, like films, TV series, etc. It is also important to recall that the USA has a very broad exclusion of broadcasting services in its own FTAs and in its GATS schedule. The broad cultural exemption Canada fought to retain in the USMCA does allow for Canadian content rules in digital media. Indeed, the text allows Canadian policy-makers to continue favouring domestic cultural industries, including publishing, film, television, news and music. In addition of this provision in the digital chapter, there is also the exception stated in Article 32.6 for the Canadian "Culture Industries". Cultural diversity is also very sensitive in countries like Australia and New Zealand. It seems therefore that many of the relevant negotiating partners have a similar approach on audio-visual services.

Is there a problem of potential discrimination on "digital products" other than those related to culture? For example on software? It does not seem to be the case. The EU takes another approach to ensuring that it undertakes wide-ranging commitments on all other transfer of data electronically transmitted. These include full FTA commitments on computer related services at a two-digit level (CPC 84). The EU also offers trading partners an article or an annex in its FTAs where parties agree on an "Understanding on computer services".

Article 212 of EU-UK TCA, for instance (last article of the Digital Trade chapter) states that the Parties agree that, for the purpose of liberalising trade in services and investment, the following services shall be considered as computer and related services, regardless of whether they are delivered via a network, including the internet:

> (a) consulting, adaptation, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, support, technical assistance or management of or for computers or computer systems;
>
> (b) computer programmes defined as the sets of instructions required to make computers work and communicate (in and of themselves), as well as consulting, strategy, analysis, planning, specification, design, development, installation, implementation, integration, testing, debugging, updating, adaptation, maintenance, support, technical assistance, management or use of or for computer programmes;
>
> (c) data processing, data storage, data hosting or database services;
>
> (d) maintenance and repair services for office machinery and equipment, including computers;

(e) training services for staff of clients, related to computer programmes, computers or computer systems, and not elsewhere classified.

EU officials are confident that this understanding covers any digital service today and in the future (… except digital audio-visual services and e-books!). EU officials are also confident that none of the digital services coming on stream on a daily basis have proved not to be covered by such a definition. This understanding has also led the EU to emphasis that the EU wants to retain the right to regulate new services, and hence does not want to take a full commitment on new services in a trade agreement. Importantly, the EU first underlines that none of the newly digitised services should be considered as "new services", since they will all be picked up in the definition of "computer related services" but nevertheless keeps the door open in case of doubt.

In the EU-Canada CETA for instance, the Annex 9-B is an "Understanding on new services not classified in the United Nations Provisional Central Product Classification (CPC), 1991". This allows the parties to introduce discriminatory regulatory requirements on "new services" that cannot be classified in the CPC (i.e. other than any other category of existing services, including other than computer related services). But should that be the case (i.e. that one of the parties would identify a "real" new service), it must notify to the other party which measure is introduced and, at the request of a party, the two (or more) countries "shall enter into negotiations to incorporate the new services into the scope of the agreement". To specify even more clearly that for the EU, the category "computer related services" is really wide ranging, this Understanding adds that, for greater certainty, the possibility for introducing discriminatory measures "does not apply to an existing service that could be classified in the CPC 1991, but that could not previously be supplied on a cross-border basis due to lack of technical facility" (this could be the case for instance for cloud services).

Would this EU method of handling the issue prove sufficiently convincing that there is no intention of introducing discrimination on digital services or "products"? Would the USA and CP-TPP countries stick to their method of automatically exempting all new services from any discriminatory treatment? It is too soon and too hard to tell. One can hope that the blockage in negotiations on this issue set at the end of the TiSA negotiations in October 2016 will be a lesson. The fact that the EU texts have not so far encountered any challenge might lead to the conclusion that the two groups of countries have the same effective objectives but go about reaching them in different ways. In the end, the result for digital trade is the same, and hence it should be possible to move on.

B. Data protection provisions in future deals? The Landing zone?

Once this issue is solved, or in parallel, the two groups will have to start negotiations on provisions on cross-border data flows and protection of personal data and privacy. We will look here at the various provisions on these two related subjects in existing treaties and see whether there are similarities, what are the impediments and absolute requirements on the part of the various parties and assess whether a final solution would be reachable at some point.

i) The principle of free flow v/s a ban on restrictions of cross-border data flows

Article 19.11 of USMCA is titled: "Cross-Border Transfer of Information by Electronic Means". Paragraph 1 states the principle:

> *"No 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".*

One can see clearly here that the conduct of business activity is the absolute priority, including possibly to the detriment of the protection of personal information… However, paragraph 2 introduces the possibility of adopting or maintaining measures inconsistent with the asserted principle that are "**necessary to achieve a legitimate public policy objective**".

The scope of a "legitimate public policy objective" can arguably be very large and include all sorts of government policies, including the protection of personal data and privacy. So one can imagine that the EU might be at ease with such a text. But the text goes on and introduces provisions in relation to the adoption of such measures.

A government can adopt measures contrary to the principle of free data flow, provided that the measure:

> *"(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or* ***a disguised restriction on trade****; and*
>
> *(b) does not impose restrictions on transfers of information* ***greater than are necessary to achieve the objective****".*

As mentioned earlier, the EU considers that the protection of personal data is a fundamental human right that cannot be made subject to any "proviso" or conditionality. A condition can always be contested. And the meaning of a "disguised restriction of trade" can be subjective. That is the reason the EU was not able to agree to such a text in the TiSA negotiations in 2016. The EU did not want its recent GDPR subject to a dispute where it might be considered as imposing restrictions on cross-border data flows "greater than necessary to achieve the objective".

One needs at this stage to go back to **GATS Article XIV**, where the protection of personal data is one of the measures specifically allowed to derogate from the GATS principle (*see above*), but it is important to recall that this article also states the following provisions:

> "*Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures…".*

Some negotiating partners therefore underline that the EU, as a signatory to the GATS, has already accepted such conditions. That is the case - the EU is bound by GATS Article XIV. And it is possible for a WTO member to complain about the EU GDPR as a disguised restriction on trade in services or an arbitrary or unjustifiable discrimination to cross border data flows. Experts close to this file will point out that it is precisely because of this potential threat that the EU could not join onto such a clause in TiSA. Nor could the EU arrive at an internal compromise (a fierce debate took place within the European Commission, and between the EU Member States), as the EU looked for alternative ways of introducing language in international treaties to ensure that data protection regulation could not be questioned.

Eventually, the EU arrived at an internal compromise in 2018 and sought to embed it in the FTAs that it was and is still negotiating. It also tabled a related text proposal in the WTO JSI

negotiations on E-Commerce on April 2019. The only text in which this alternative proposal to the USMCA/CP-TPP is now enacted is **Article 201 of the EU-UK TCA**, where it is stated:

> *"The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party: …"*.

The text then lists four possible different ways of restricting data flows, such as requiring the use of computing facilities, requiring localisation of data in the Party's territory for storage or processing, etc. In order to remain open to the fact that this list would not be exhaustive, paragraph 2 introduces a review clause and rendezvous clause in three years after the entry into force of the agreement. The EU argues that the sentence "cross-border data flows shall not be restricted …" and its following paragraph, introduces obligations as strong as the principles asserted in USMCA. It seems however that this view is not fully shared by other trading partners, including parties to the CP-TPP and the USA. The more fundamental problem might lie in the following article of the EU proposal.

ii) Carve-out of safeguards for protection of personal data v/s Recommendations to protect personal data

It needs first to be emphasised that the notion of cross-border data flows covers **all data, i.e. personal data and non-personal data,** including data in the financial services sectors at large, and all the anonymised data flowing from machine-to-machine, Internet of things, Artificial Intelligence, etc. Improving international governance for these digitally enabled services is vital for companies and crucial for development and innovation in these sectors.

In this context, it is interesting to remember the figures released by UNCTAD in 2019. The value of worldwide e commerce was assessed at US$ 29 trillion in 2017, **88% of which were B2B** and only 12% B2C operations. So the personal data protection regulations target only around 10% of all data! As a quick aside, some member countries and institutions of the EU now appear willing to introduce data protection rules also on "non-personal" data. This is an important space to watch in the coming months.

Returning to text in trade agreements, the USA and the CP-TPP countries do have language on "data protection". Article 19.8 ("Personal Information Protection") of the USMCA for instance states in paragraph 1:

> *"The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade."*

Clearly, the focus is on the economic benefits, including for consumers. There is no dimension here regarding the protection of the "citizen". Paragraph 2 establishes an obligation to put into place a regulation:

> *"To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade".*

It then indicates the signatories "should" take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

This should be welcomed by the EU, as the issue of protection of personal data is taken seriously by other trading partners. The EU considers, however, that this language on data

protection is very weak, even if it refers to APEC or OECD privacy rules since they are not binding, and hence very far from what the EU considers relevant to a fundamental human right.

For its part, the EU has tabled a proposal to its trading partners for an article entitled "Protection of personal data and privacy" (see for instance the proposal to Australia here). It states that:

> *"1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade."*

One can see here the reference to "fundamental right", however such a recognition or lack of recognition is not a problem in itself. The main issue here is the high standard of protection. The problem lies in the second paragraph which states:

> *"2. Each Party **may** adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, **including** through the adoption and application of **rules for the cross-border transfer** of personal data. **Nothing in this agreement** shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."*

Australia and the CP-TPP countries consider that the language proposed by the EU is too protective regarding data privacy regulation, and fear that such language would allow abuse to disguise data localisation requirements, hence limiting the flows of data across borders. The EU argues that the objective is solely to allow regulation for data protection purposes, and hence added a third paragraph obliging the signatories to inform the other party of any safeguard it adopts or maintains, with the view that if one of the parties considers that a proposed measure has a larger scope (disguised localisation under the pretext of protection of personal data), that measure can be contested. Clearly the EU proposal is having difficulties in getting through. But EU negotiators have been obliged to stick to this language given that it took more than two years internally to achieve this compromise.

iii) EU-UK TCA data protection safeguard subject to transfer mechanisms

One major event has happened that finally opened the door to smoother language: Brexit and the negotiation of the EU-UK TCA. The UK negotiators, with full awareness of internal EU procedures, sought nevertheless to introduce some changes to the EU text. And those that finally were accepted might represent a possible landing zone with other trading partners as well, such as Australia or New Zealand, and possibly in the JSI E-Ecommerce negotiations.

First, in paragraph 1 of Article 202 of the EU-UK TCA, there is no longer any reference to "fundamental right" which is replaced by recognition that "individuals have the right to the protection of personal data…". Second, the strong carve-out (starting with "Nothing in this agreement…") is still there at the beginning of the second paragraph of Article 202, but for the first time the EU accepted some conditionality. The new sentence "**provided that the law of the Party provides for instruments enabling transfers under conditions of general application (1) for the protection of the data transferred"** has been introduced.

This somewhere barbaric language for non-experts is a means of expressing the fact that the EU does indeed have strong GDPR provisions that have an extraterritorial effect, but the GDPR does not prevent cross-border data flows from taking place. It does not, therefore, impose any obligation to localise in EU territory. On the contrary, the regulation put into place some

transfer mechanisms that, when respected by operators, allow them to have access to and process data of EU citizens outside the EU. These mechanisms are detailed in Article 44, 45 and 46 of GDPR (Chapter V: Transfer of personal data to third countries or international organisations). These mechanisms are for instance the **adequacy decision** of national legislation on data protection. Such decision is granted by the EU after assessment of that national law. It has been granted for instance to Canada, Japan, New Zealand and more recently to the UK. There are other mechanisms called "appropriate safeguards" that are put into place by operators/companies and hence will not require from them any specific authorisation from a supervisory authority. These are the EU Binding Corporate Rules (**BIC**) or the Standard Contractual Clauses of the EU (**SCC**). We will not dive into this system here.

One must admit that the footnote aimed at explaining the meaning of "conditions of general application" does not help but rather confuses the reader:

> "footnote 1: *For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases".*

What this actually means is that the transfer mechanisms must be applied by all companies willing to transfer data; either thanks to the national law recognised as adequate, or thanks to specific contractual clauses used by a given company that fulfil criteria recognised as sufficient to protect the data of EU data subjects, or thanks to so-called SCCs that are pre-approved by the European Commission.

On 4 June 2021, the Commission issued modernised SCCs under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46.

The main element to take into consideration here is that the full carve-out has been modified by the fact that any country which would want to adopt data protection measures cannot do so if it does not put into place transfer mechanisms that would allow data to flow across the borders. Personal data protection can no longer, therefore, be used as a disguised barrier to cross-border data flows such as introduction of localisation requirements.

5. Conclusion

Should the countries of the first block mentioned earlier in this paper consider this EU proposed requirement of establishing transfer mechanisms within data protection regulation as acceptable - framing the regulatory power of a party so that it is actually limited to personal data protection and providing ways to continue to transfer data across borders - one would hope that these 12 countries would be joined by the EU and other like-minded countries to move ahead and adopt the first ever plurilateral framework of rules on cross-border data flows.
