Australian and New Zealand Journal of European Studies
https://esaanz.org.au/anzjes/
Vol13 (2)
ISSN 1837-2147 (Print)
ISSN 1836-1803 (On-line)

The Regulation of personal data flows between the European Union and the Asia-Pacific Region

ANA GASCÓN MARCÉN
University of Zaragoza, Spain
angascon@unizar.es

Abstract
This paper explains the legal framework for cross-border transfers of personal data outside the EU and assesses its impact on a selection of Asia-Pacific data protection laws. It studies the position defended by the EU in the debates for a new general framework on e-commerce in the World Trade Organization (WTO) and the sections regarding data flows of some free trade agreements recently concluded by Asia-Pacific countries such as the Regional Comprehensive Economic Partnership and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. This paper shows how the regulation of data flows has surpassed national data protection laws to be increasingly present in free trade agreements with the tensions this may entail, paying special attention to the EU and Asia-Pacific. A holistic view is necessary because the consequences for human rights in trade negotiations should not be overlooked.

Keywords: Asia-Pacific, Electronic Commerce, European Union, GDPR, personal data flows

Introduction

The significance of digital trade and the centrality of data for economic processes, both as a contribution to economic growth and as a preoccupation of governments with digital trade-related policies, have grown exponentially in the last years (Burri, 2017). The European Union (EU) and several countries of Asia-Pacific, such as China or Japan, have been very vocal in presenting their positions about data flows and trade, a topic that gains importance every day in the international sphere.

The issue of free flow of personal data is essential to reach the full potential of free trade agreements (FTAs), especially for e-commerce. There is currently a tendency to include digital trade chapters in these treaties that deal with the regulation of cross-border data flows or data localisation. These topics are highly controversial among different stakeholders. While the EU considers personal data protection a fundamental right[1] and wants to ensure the free flow of data with privacy safeguards, China desires to unbundle human rights questions from trade discussions and legitimise its data localisation laws based on national security reasons. There is a clear trend to regulate data flows not just in data protection laws but also trade agreements and this may have

[1] The protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights of the EU.

an impact on human rights, as the objectives of those sets of rules have been traditionally different.

In this scenario, it is interesting to look at how Asia-Pacific countries are tackling these questions both in their national data laws, which are evolving and flourishing, but also in their FTAs. The importance of these countries in the trade sector is increasing so they can be a force that turns the scale towards one side or another at the global level and align themselves with the European or the Chinese approach.

This paper presents the legal framework for cross-border transfers of personal data outside the EU (II) to show later its impact on a selection of Asia-Pacific data protection laws (III). As the regulation of data flows has surpassed data protections laws, this article looks at the trend to regulate data protection flows in FTAs. It presents the position defended by the EU in the World Trade Organization (WTO) around the debates on e-commerce (IV) and explains how the FTAs concluded recently by the Asia-Pacific countries regulate this topic (V).

The legal framework for cross-border transfers of personal data outside the EU

The General Data Protection Regulation (GDPR) establishes that a controller or processor may transfer personal data to a third country only if they provide appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies are available. The appropriate safeguards can be provided by: binding corporate rules, standard data protection clauses (SCCs), codes of conduct, or certification mechanisms. There are also some derogations for specific situations, for example, when the data subject has explicitly consented to the proposed transfer, after being informed of the possible risks of such transfers, but these derogations are the exception and should only be used for occasional and not repetitive transfers.

The best option for the businesses of a third country is to get an adequacy decision. A transfer of personal data to a third country may take place when the Commission has decided that it ensures an adequate level of protection. This level of protection should be essentially equivalent to the one guaranteed within the EU, according to the Court of Justice of the EU (CJEU) in its *Schrems* judgement.[2] To issue an adequacy decision, the Commission assesses the relevant legislation and its implementation, the access of public authorities to personal data, the rules for the transfers to a third country, the data subject rights and redress mechanisms, the existence of effective and independent data protection authorities, and the international commitments of the third country.

The European Commission has adopted adequacy decisions for countries such as Andorra, Argentina, Canada, Israel, Switzerland or Uruguay. From the Asia-Pacific, only Japan and New Zealand have one, although, the negotiations with South Korea have finished and India has shown its desire to get one. An adequacy decision is the most advantageous option for the businesses, especially medium and small ones, because it frees the personal data flow and they do not have to use any of the specific mechanism mentioned above.

[2] CJEU Judgment, 6 October 2015, Maximillian Schrems v. Data Protection Commissioner, C- 362/14.

This is one of the reasons why states across the globe are adopting data protection laws and converging with the GDPR, a gold standard in the field. In the decade 2010-2019, 62 countries enacted such laws, more than in any previous decade, representing a total of 142 countries with them at the end of 2019 (Greenleaf & Cottier, 2020).

Lacking an adequacy decision, the instrument most widely used to cover cross-border personal data transfers are SCCs. These are standard sets of contractual terms and conditions approved by the Commission that offer the additional safeguards asked by the GDPR. This used to be the easiest mechanism because it sufficed to copy-paste the text in the contracts between the sender and the receiver of the data to be covered. Nevertheless, it has become a lot more difficult after the *Schrems II* judgement of the CJEU[3]. In this judgement, the Court clarified that data subjects whose personal data are transferred to a third country pursuant to SCCs must be afforded a level of protection also essentially equivalent to that guaranteed within the EU.

The assessment of that level of protection is quite cumbersome and has to be done by any business (big or small) that wants to send data to a third country. An assessment of each country to which they want to send data is needed and it has to take into account not just the data protection law of the country, but also surveillance practises, enforcement mechanisms, etc. This is quite difficult. As an example, when the Commission does one to issue an adequacy decision it takes years, moreover, the two times those assessments have been brought before the CJEU, it has invalidated both. Now, according to the Court, any company that wants to use SCCs should do those assessments.

This may prevent data transfers to many countries, if the assessment is done according to the stringent guidelines approved by the European Data Protection Board following the judgment. In practice, this makes impossible to use SCCs (and probably all the other mechanisms mentioned) for transfers to countries such as China or India, because of the access of public authorities to data without human rights safeguards and the lack of recourse mechanisms. To have an idea of how this can affect data flows with the Asia-Pacific, a general overview will follow of some of their data protection laws.

Data protection laws in the Asia-Pacific region and the GDPR

It is beyond the scope of this article to assess the level of personal data protection in all the countries of Asia-Pacific. Only a brief overview of a few of the most significant and representative ones is presented. This will highlight the impact of the GDPR in these laws. They have recently evolved and regulated topics that are entering the legislative realm of FTAs, such as data export limitations or data localisation.

Japan's Act on the Protection of Personal Information (APPI) was amended in 2015 and 2020 to further converge with the GDPR. One of its advances was the creation of an independent data protection authority in 2016 (the CPIP), although it only covers the private sector. There were some discrepancies between the APPI and the GDPR that made necessary the adoption in 2018 of Supplementary Rules for the Handling of Personal Data Transferred from the EU. This made possible the adequacy decision for the private sector of Japan. However, some authors argued that Japan does not offer an equivalent level of protection (Greenleaf, 2018) and that this decision was motivated

[3] CJEU Judgment, 16 July 2020, Data Protection Commissioner v. Facebook Ireland, Maximillian Schrems, C-311/18.

by an economic imperative to reach the full potential of the Economic Partnership Agreement between the EU and Japan that entered into force immediately afterwards (Kanetake & de Vries, 2018). Japan established in the APPI a system that limits personal data flows to third countries unless there is informed consent of the data subject or the CPIP declares that that country has a level of protection equivalent to that of Japan. This resulted in mutual decisions of adequacy between the EU and Japan in 2019.

New Zealand has had an adequacy decision since 2012. This status gives it an economic advantage over neighbouring Australia. As this decision is under revision, New Zealand adopted a Privacy Bill that updated its Privacy Act in 2020. This Bill introduced changes to converge with the GDPR: mandatory data breach reporting, restrictions on offshore transfers of personal information and clarifications on the extraterritorial scope of the Act.

Australia asked for an adequacy decision in 2001. Eight areas in which its law did not offer adequate protection for personal data were identified. However, the Australian Government declined to revise the laws to meet the required standard. Australian laws have been amended in the meantime, for example, creating data breach notification obligations in 2017. However, Kemp and Greenleaf (2020) consider that Australia is still far behind international standards and, until some needed reforms occur, it would be pointless to try to obtain an EU adequacy decision.

China is viewed as a country with a low level of data protection. This is due to several factors, such as its Social Credit System, which according to Greenleaf (2019a) is emerging as the world's most pervasive and potentially totalitarian surveillance system and entails mayor risks for human rights. However, China presented a draft of a Personal Information Protection Law for public consultation in 2020. The draft contains several articles inspired by the GDPR, such as the one on extraterritorial application. Nevertheless, it also contains others that reinforce the divergences, such as stronger data localisation. The draft law proposes a more expansive data localisation requirement compared with the existing one in China's Cybersecurity Law. Furthermore, processors over a certain threshold would need a security assessment by the Chinese regulators for any cross-border data transfer.

South Korea finished negotiations for adequacy in 2021. The Korean personal data protection regime is one of the strictest in the world. In 2020, South Korea enacted amendments to its major data protection laws. Its framework became closer to the GDPR, for example, regarding the creation of a real independent enforcement authority and safeguards for the cross-border transfer of personal information: restricting the onward transfer of personal information and making necessary to appoint a local representative.

Thailand's Personal Data Protection Act of 2019 is one of the strongest data privacy laws in Asia and the first explicitly 'GDPR-based' law enacted in the region. A substantial set of the innovations of the GDPR principles are included but unfortunately not all (Greenleaf & Suriyawongkul, 2019). India presented a Personal Data Protection Bill in 2019 not yet passed into law. It has been widely inspired by the GDPR, but it incorporates data localisation clauses and a complex system for data exports (Greenleaf, 2020a). In 2020, Indonesia discussed a Personal Data Protection Bill inspired by the GDPR that may be enacted in 2021, while other laws in Indonesia

establish a data localisation regime. Bhutan and Nepal enacted privacy laws in 2018, but they do not include most of the principles of the GDPR (Greenleaf, 2019). In 2019, Sri Lanka launched a draft bill for an Act for the Regulation of Processing Personal Data and, in 2020, Pakistan published a consultation draft of a Personal Data Protection Bill. Currently, both lack a general data protection law.

There is a wave of new data protection laws and reforms in the Asia-Pacific. Nevertheless, the freedom of those states to regulate data protection flows to third countries and data localisation in their national laws may be constrained in the future, as clauses regarding those questions have been included in some recent FTAs.

The European Union's approach to the free flow of data in free trade negotiations

The increasing importance of personal data flows for electronic trade has made this topic a domain to which the negotiators of FTAs have started to pay attention. That is the reason why we study how the regulation of cross-border data flows is incorporated into FTAs and debates on a possible international framework.

The WTO is the natural framework to discuss such matters. It had a work program on e-commerce since 1998 but failed to adopt general rules. Several countries presented a Joint Statement Initiative at its Ministerial Conference in 2017, followed by another in 2019 that brings together 83 states to discuss a possible international agreement on e-commerce. Japan, Australia and Singapore are the co-conveners of this initiative, showing the leadership of Asia-Pacific in such endeavour.

The EU has defended at the WTO that states should be committed to ensuring cross-border data flows to facilitate trade and data localisation requirements should be banned. Some of the reasons used by states to justify data localisation laws are to assist law enforcement and national security agencies' access to data; to provide geo-political advantages; to ensure government access to certain categories of data; and to provide economical competition advantages (Svantesson, 2020). Nevertheless, it may also have negative consequences. Plaum (2014) explains that it entails several risks because, through these measures, a government can increase control over its residents' online activities, raising the possibility of abuse and putting at risk citizens' right to privacy and freedom of expression, targeting dissidents and forcing jurisdiction. Freedom House (2020) argues that domestic data storage requirements place users' data firmly in the legal purview of governments, significantly enhancing authorities' surveillance capabilities by lowering access barriers to this data. It highlights the risks for privacy, freedom of expression, access to information, press freedom, freedom of belief, non-discrimination, freedom of assembly and association and due process.

The EU restricts cross-border personal data flows because the protection of personal data and privacy are fundamental rights. That is why it has defended at the WTO that states may adopt and maintain the safeguards they deem appropriate to ensure the protection of privacy, including through the adoption and application of rules for the cross-border transfer of personal data (such as the ones of the GDPR). For that purpose, the EU created horizontal dispositions in 2018 to incorporate in FTAs to ban data localisation but allow restrictions to protect privacy. This is not data localisation because it does not create the obligation to store data in the territory of a State; instead, it makes sure that safeguards travel with the data. These dispositions are the tool that

the EU uses to balance its data protection obligations with its support for free trade and its commitments under WTO Law (Irion, Yakovleva & Bartl, 2016).

The negotiations on e-commerce at the WTO have reached a consensus on subjects such as spam, electronic contracts, protection of online consumers and electronic authorization and signatures. Nevertheless, there is still controversy around data flows, data localisation, privacy, transfers of source code, internet taxes and censorship.

The EU's free trade negotiations with the Asia-Pacific states are a good example of how data flows have gained importance and the EU position has evolved. The Agreement with South Korea (2010) was meagre in respect of e-commerce. It forbids customs duties on deliveries by electronic means and asks for cooperation on some regulatory issues. The Agreement for an Economic Partnership with Japan (2018) had a fully developed chapter on e-commerce. Japan wanted to add a free data flow clause to it, but the EU preferred to manage it through an adequacy assessment. Japan only succeeded in obtaining a promise in an article to reassess in three years the need for inclusion of provisions on the free flow of data.

The European Commission is negotiating FTAs with New Zealand and Australia. In its directives, the Council of the EU has stated that the negotiations should result in rules covering digital trade and cross-border data flows and unjustified data localisation requirements (among others), while respecting the EU's personal data protection legislation. In the EU proposals for the digital trade titles, the EU has used the horizontal provisions that recreate its position for the WTO negotiations.

New Zealand and Australia broadly agree with the EU on these topics. Australia in its negotiation's aims has stated that it is seeking to establish ambitious digital trade commitments that strike a balance between facilitating modern trade and ensuring appropriate protections for consumers. Because high-quality rules on issues such as data flows and localisation will create a more certain and secure online environment and support increased growth of e-commerce between Australia and the EU.

New Zealand seeks a broad, high-quality e-commerce chapter with the EU that will allow businesses to freely transfer data and protect the privacy and rights of consumers. The EU will not agree to make the free flow of personal data a binding obligation of the agreement. The FTA will just include the commitment of both parties to maintain a high degree of data protection but the specific mechanism to allow the free flow of data will still be an adequacy decision system following the GDPR. The result in practice is the same, although the Commission can unilaterally revoke any adequacy decision.

We can see a high level of convergence between Japan, South Korea, Australia, New Zealand and the EU. They believe in free trade coupled with human rights protection and may form a front for example in the WTO to face other approaches to trade such as the Chinese one, that wants to unbundle trade from human rights issues and to defend data localisation as a national security question.

It would be even better if those countries could also count on the support of the USA (a natural ally in many other fronts), but this country does not condition free trade to strong privacy safeguards, as it does not have a general data protection law. Australia, Japan, New Zealand, South Korea, the EU and other countries with a similar view can

offer a third way from the USA (Silicon Valley's) libertarianism and China's techno-authoritarianism.

New developments in Asia-Pacific trade agreements concerning data flows

It is also relevant to look at what Asia-Pacific countries are currently including it their FTAs beyond the ones with the EU. Asia-Pacific states such as Japan, New Zealand or Singapore have recently adopted some of the most advanced and developed agreements focused on digital trade, such as the USA-Japan Agreement on digital trade and the Digital Economy Partnership Agreement (DEPA). Simultaneously, two multilateral agreements have been negotiated with the aim of involving a huge number of countries of the region, the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Even if these agreements are less ambitious, they show what is achievable in the field of data flows with a higher number of less homogenous States and may give some ideas of possible compromises at the WTO.

The USA-Japan Agreement on digital trade entered into force in 2020. It is one of the first agreements in the world focused only on digital trade and it is more detailed than most chapters on digital trade of FTAs. The parties are economic superpowers with leading digital businesses and with a lot of influence on future multilateral negotiations.

The USA-Japan Agreement establishes that neither 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. Nevertheless, nothing shall prevent a Party from adopting or maintaining a measure that is necessary to achieve a legitimate public policy objective, provided that the measure: is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and does not impose restrictions on transfers of information greater than are necessary to achieve the objective. These conditions are similar to the strict test formulated by the GATS and the GATT and have as an objective a test to balance trade and nontrade interests by creating certain exemptions.

Japanese data protection law limits cross-border data flows in a similar way to the GDPR and the scheme to send personal data form the EU to the USA has been annulled twice by the CJEU because of the lack of the necessary safeguards in the USA legislation. Nevertheless, Japan still decided to commit to free data flows in this international agreement superseding in a certain way its own legislation. This is not surprising considering the USA's influence over Japan.

The Agreement also bans data localisation because it establishes that neither Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business, although there is an exception for financial service suppliers. There was not much risk of data localisation in any of the states, this is mostly a disposition of principle to show their oppositions to such laws used, for example, by China (but not only).

Abe Shinzo proposed the concept of *Data Free Flow with Trust* at the World Economic Forum in 2019. Japan took advantage of the G20 meeting it hosted that year to launch the Osaka-Track. This initiative that continued the previous one aims to standardise the rules for e-commerce and the global movement of data flows with better protection for privacy, intellectual property and cybersecurity. The EU, the USA, China and 21 other States formally signed the Osaka Declaration on Digital Economy, which commits the signatories to promote efforts in the development of international standards in this area. However, other relevant states decided to stay out, such as India or Indonesia. India favours data localisation, reflecting the Modi government's policy that data is a national asset, not primarily an individual right, as set out in its e-commerce policy (Greenleaf, 2019).

Turning to other Asia-Pacific states, the DEPA is an agreement signed by Singapore, Chile and New Zealand in 2020.[4] This agreement does not limit itself to cover trade but goes further, promotes interoperability between different regimes and addresses the new issues brought about by digitalisation. It is structured around different modules that may be imitated in other agreements, and it was done with a broader intention as it is open to WTO members that are able to meet its standards. Canada has already shown its willingness to join it.

The DEPA has a module dedicated to data issues. The Parties should adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. They even list some of the principles that should underpin these frameworks such as collection limitation, data quality, and purpose specification or use limitation. They recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. Nevertheless, they 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. The possibility of exceptions has the same limitations as the USA-Japan Agreement.

Each Party may also have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. No Party shall require a covered person to use or locate computing facilities in its territory as a condition for conducting business in that territory. Nevertheless, a Party may adopt or maintain measures to achieve a legitimate public policy objective, provided that they are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and do not impose restrictions greater than the ones required to achieve the objective. This again applies the four-step test of the GATS and the GATT, in this case not only to the restrictions on data flows but also to data localisation measures.

Another important FTA signed by Asia-Pacific countries recently is the CPTPP between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.[5] Even if the USA is not a party to this agreement, it had a great influence in its drafting, as this treaty contains most of the dispositions of the Trans-Pacific Partnership (TPP) negotiated by the US and later rejected by the Trump

[4] In December 2020, Canada requested exploratory discussions to join the DEPA. Australia and Singapore also have a Digital Economy Agreement (DEA), which entered into force in December 2020 that follows along the same lines.

[5] The UK requested to join the CPTPP in February 2021 and the formal negotiations were set to start throughout the year.

administration. This Agreement is important because of its number of members, their relevance and its ambitious goals in dismantling trade barriers. While it has a high number of members, they are less heterogeneous that the RCEP.

Regarding digital trade, the CPTPP establishes that each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of e-commerce. In its development, each Party should take into account the principles and guidelines of relevant international bodies. Unfortunately, the CPTPP does not specify these principles. It opts to permit a very low standard when clarifying that a Party may comply with this obligation by adopting or maintaining measures such as comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, but also laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy. Regarding data flows, it uses the same dispositions as the Japan-USA Agreement and the DEPA, and it bans data localisation as described in the DEPA, only in this case the dispositions apply to many more countries, including Vietnam, which has a data localisation law.

Burri (2021) considers that these provisions illustrate an interesting development because they do not simply entail a clarification of existing bans on discrimination, nor do they merely set higher standards, as it is anticipated from FTAs. Instead, they concentrate on shaping the regulatory space domestically. Nevertheless, Greenleaf (2020b) considers that the agreements with CPTPP-inspired clauses create a great likelihood of inconsistency and conflict with the EU adequacy requirements of export limitations and the increasing number of Asian data privacy laws with broad mandates for data localisation. Streinz (2019) argues that the CPTPP parties endorsed the Silicon Valley Consensus of uninhibited data flows and permissive privacy regulation (which the USA incorporated in the TPP) due to a lack of alternatives and persistent misperceptions about the realities of the global digital economy, partly attributable to the dominant digital trade framing. He suggests the need for a new approach for the inclusion of data governance provisions in future FTAs that offers more flexibility for innovative digital industrial policies and experimental data regulation.

Notwithstanding the importance of the CPTPP, probably the FTA among Asia-Pacific countries that has garnered more attention recently is the RCEP, signed in 2020 between Australia, Brunei, Cambodia, China, Indonesia, Japan, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, South Korea, Thailand and Vietnam. These countries account for 30% of the world's Gross Domestic Product, creating the world's largest trading bloc. It is the first FTA between Japan, China and South Korea. India participated in the negotiations, although it opposed the digital trade chapter, and finally did not sign the treaty.

The RCEP covers almost the whole Asia-Pacific, but the heterogeneity of its parties makes it less ambitious than the above-mentioned treaties. However, it has a chapter dedicated to e-commerce. Its drafting may seem similar to the CPTPP, but the slight differences have important consequences.

A Party shall not prevent cross-border transfers of information by electronic means where such activity is for the conduct of the business of a covered person. Nevertheless, nothing shall prevent a Party from adopting any measure that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable

discrimination or a disguised restriction on trade; or any measure that it considers necessary for the protection of its essential security interests. The other Parties cannot dispute such measures. The same applies to the localisation of computing facilities. The divergence from the CPTPP drafting means that a very wide margin for action is given to states because they decide what is necessary to achieve a legitimate policy or the protection of their essential security interests. In addition, a conflict over the application of these articles cannot be submitted to the dispute settlement mechanism of the RCEP, which makes them unenforceable.

Leopold (2020) considers that China, which tightly protects its digital realm from the outside world, was behind such weakening language and ensured that the RCEP would allow it to keep its Great Fire Wall intact. Novi (2019) and Kelsey (2017), on the other hand, criticise the ambition of the treaty, considering this model of e-commerce could impede the development of the ASEAN countries, create negative fiscal and employment consequences and leave them dependent on an oligopoly of private corporations that control the global digital infrastructure and mass data. They consider that ASEAN countries will need to resist those proposals if they are to maintain their regulatory sovereignty and the policy space to capitalize on the 21st century digital revolution.

The selection of FTAs assessed shows what is possible to achieve for countries with broadly similar views. It is easier to reach detailed agreements on digital trade, ensure data flows and reject data localisation requirements. When the number of countries and their heterogeneity increases, the agreements are less granular and have to accommodate exceptions, such as those of the CPTPP. This is exacerbated when influential players with a different approach join the negotiating table, as it is the case of the RCEP and China.

Finally, even if some of these treaties underline the importance of privacy, it is just to pay lip service to it as not binding specific obligations or real standards are created. There is no universal international treaty for the protection of personal data, but the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is open to non-European States. There is no party yet from Asia-Pacific but South Korea could be a good candidate.

Conclusions

The influence of the GDPR on Asia-Pacific laws, with a continuous reinforcement and enactment of new laws in recent years, shows the global impact of this regulation. However, this convergence may not be enough for the EU. If we add to the restrictions on cross-border personal data transfers of the GDPR the interpretation of the CJEU in *Schrems II*, personal data exports are going to become extremely complex. This is because of the added burdens to use SCCs, the extra difficulty to grant adequacy decisions and the ban to send data to some countries where the authorities have unfettered access to it.

The EU supports the liberalisation of trade but only as long as it is able to safeguard its core values such as workers' rights or the protection of the environment and, obviously, personal data protection. This is the reason for its proposals at the WTO as well as its horizontal provisions for FTAs. This approach to negotiations with Japan, New Zealand or Australia does not seem controversial but blocks the possibility of an FTA with China.

The EU will pay special attention to the developments in the Asia-Pacific regarding data flows as some of these countries are adopting the most developed agreements on digital trade, the USA-Japan Agreement and the DEPA are good examples of this trend. It is also important to assess the e-commerce chapters of the CPTPP and the RCEP. All of them have bans on data localisation and support the free flow of data, but their exemptions are different. Especially, the dispositions of the RCEP leave such a wide margin of appreciation to states that the relevant dispositions are almost meaningless. However, these articles can very well be the blueprint for the WTO negotiations.

The increasing number of data protection laws in Asia-Pacific may seem proof of a mounting interest in privacy. Nevertheless, the FTAs tell a different story. They underline the importance of privacy but without binding standards. The stated objective in all the digital trade chapters of the agreements studied from that region is the free flow of data. This is positive if it goes hand in hand with an effective privacy framework, because if not it means sacrificing fundamental rights for economic reasons. This is the position the EU should defend at the WTO together with states such as Japan, South Korea, New Zealand or Australia. Electronic commerce is going to become even more important in the future, so the EU has to make sure that it can continue protecting personal data and at the same time keeping its international commitments. At the end the free flow of data cannot just be enabled for economic purposes, this is why the data flows between the EU and Asia-Pacific have to take into account the particular situation of each of the countries in the region.

The whole world should monitor and evaluate the results in practice of the Asia-Pacific agreements and assess the consequences to their state parties in economic but also personal data protection terms, as their objectives should not just be to increase trade but also to improve the lives of their constituents.

References

Andersen, H. (2015). Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions, *Journal of International Economic Law* 18, 383-405.

Burri, M. (2017). The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. *UC Davis Law Review* 51, 65-132.

Burri, M. (2021). Towards a New Treaty on Digital Trade. *Journal of World Trade* 55 (1).

Campbell, K. & Andrews, B. (2013). *Explaining the US 'Pivot' to Asia*. Chatham House. https://kritisches-netzwerk.de/sites/default/files/explaining_the_-us_pivot_to_asia_-_kurt_campbell_and_brian_andrews_-_the_asia_group_-_august_2013_-_9_pages_0.pdf

Freedom House (2020). *User privacy or cyber sovereignty? Assessing the human rights implications of data localization*. https://freedomhouse.org/sites/default/files/2020-07/FINAL_Data_Localization_human_rights_07232020.pdf

Greenleaf, G. (2018). Japan: EU Adequacy Discounted. *Privacy Laws & Business International Report* 155, 8-10.

Greenleaf, G. (2019a). Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock. *Revista Uruguaya de Protección de Datos Personales* 4, 49-73.

Greenleaf, G. (2019b). Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal. *Privacy Laws & Business International Report*, 22-25.

Greenleaf, G. (2020a). India's Data Privacy Bill: Progressive Principles, Uncertain Enforceability. *Privacy Laws & Business International Report* 163, 6-9.

Greenleaf, G. (2020b). Will Asia-Pacific trade agreements collide with EU adequacy and Asian laws? *Privacy Laws & Business International Report* 167, 18-21.

Greenleaf, G. & Suriyawongkul, A. (2019). Thailand-Asia's Strong New Data Protection Law. *Privacy Laws and Business International Report* 160, 3-6.

Greenleaf, G. & Cottier, B. (2020). 2020 Ends a Decade of 62 New Data Privacy Laws. *Privacy Laws & Business International Report* 163, 24-26.

Kanetake, M. & de Vries, S. (2018). EU-Japan Economic Partnership Agreement: Data Protection in the Era of Digital Trade and Economy. *RenforceBlog*. 18/12/2020. http://blog.renforce.eu/index.php/en/2018/12/18/eu-japan-economic-partnership-agreement-data-protection-in-the-era-of-digital-trade-and-economy/

Kelsey, J. (2017). *The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of e-Commerce*, ERIA Discussion Paper Series, https://www.eria.org/ERIA-DP-2017-10.pdf

Kemp, K. & Greenleaf, G. (2020). Competition and Consumer Watchdog Spurs Australian Privacy Changes. *Privacy Laws & Business International Report* 167, 25-28.

Leblond, P. (2020). Digital Trade: Is RCEP the WTO's Future? *CIGI online*, 23/11/2020 https://www.cigionline.org/articles/digital-trade-rcep-wtos-future

Novi, E. (2019). The Risk of E-Commerce Provisions in the RCEP, *The Diplomat*, 4/4/2019 https://thediplomat.com/2019/04/the-risk-of-e-commerce-provisions-in-the-rcep/

Plaum, A. (2014). The impact of forced data localisation on fundamental rights. *Access Now*. 4/6/2014 https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/

Streinz, T. (2019). Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy. *Megaregulation Contested: Global Economic Ordering After TPP*, Oxford University Press, 312–342.

Svantesson, D. (2020). *Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines*, OECD.